Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364
*Interim Class Counsel*

**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF CALIFORNIA**
**SAN JOSE DIVISION**

| | |
|---|---|
| IN RE IPHONE APPLICATION LITIG. | CASE NO. 5:11-MD-02250-LHK<br>JURY DEMAND<br>FIRST AMENDED, CONSOLIDATED CLASS ACTION COMPLAINT FOR VIOLATIONS OF:<br>1. STORED COMMUNICATIONS ACT, 18 U.S.C. § 2701;<br>2. ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. § 2510;<br>3. CALIFORNIA CONSTITUTION, RIGHT TO PRIVACY, ART. I, SEC. 1;<br>4. NEGLIGENCE;<br>5. COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030;<br>6. TRESPASS;<br>7. CONSUMERS LEGAL REMEDIES ACT, CAL. CIV. CODE § 1750;<br>8. UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200;<br>9. CONVERSION; and<br>10. COMMON COUNTS, ASSUMPSIT, AND UNJUST ENRICHMENT/RESTITUTION |

The persons designated below as Plaintiffs ("Plaintiffs"), each on his or her own behalf and, collectively, on behalf of all others similarly situated (the putative "Classes"), make the following allegations against Apple Inc. ("Apple") and the other Tracking Defendants named below, which allegations are made based on each Plaintiff's personal knowledge of his or her own acts and observations and, otherwise, upon information and belief based on investigation of counsel. To the extent the Complaint refers to actions directed at Plaintiffs, such allegations also refer to actions directed at the Class Members as well.

## I. NATURE OF CASE

1. During the Class Period, each Plaintiff named herein had personal data collected from their iDevices while using Apple-approved Apps. Such data was identifiable as to each of the Plaintiffs and was transmitted to third parties for purposes wholly unrelated to the use and functionality of their iDevices or the Apps contained thereon.

2. None of the Plaintiffs was made aware of or consented to the taking of this data, and there was no way to opt out of this surreptitious, third-party collection of information. The information collected included but was not limited to: a Plaintiff's precise home and workplace locations and current whereabouts; unique device identifier (UDID) assigned to Plaintiff's iDevice; personal name assigned to the device (e.g., "Beth's Phone"); Plaintiff's gender, age, zip code, and time zone; as well as App-specific activity such as which functions Plaintiff performed on the App; search terms entered; and selections of movies, songs, restaurants or even versions of the Bible.

3. As a result, each of the Plaintiffs had the resources of their iDevice consumed and diminished without their permission. Such resources were measurable and of actual value, and included iDevice storage, battery life, and bandwidth from each Plaintiff's wireless services provider. The monetary value of the resources taken from Plaintiffs is quantified below.

4. The transmission of personal information to third parties employed such substandard security measures that it exposed each Plaintiff to unexpected and unreasonable risks of the interception of their personal information. Such poor security practices of the iDevices were contrary to specific representations made about the iDevices at the time of Plaintiffs' pur-

chases and contrary to standard, expected practices.

5. Among other injuries and damages detailed herein, had Plaintiffs known of the above-summarized characteristics of the iDevices during the class period, Plaintiffs would not have purchased iDevices or, certainly, would not have paid what they did for devices that were substantially devalued by the undesirable characteristics inextricably linked to the devices and their operating environment.

6. This Complaint details these allegations, the statutory and common law remedies Plaintiffs seek for these wrongs, including injunctive remedies and accountability for those entities responsible.

## II. INTRODUCTION

### A. Apple Charged Each Plaintiff a Hidden Premium in the iDevice Purchase Price.

7. Plaintiffs each purchased iPhones—which are expensive among cell phones in the market—for prices ranging from $199 to $399, as detailed more fully below.

8. The purchase price of Plaintiffs' iPhones included access to thousands of purportedly free third-party software applications ("Apps") available in Apple's App Store.

9. Each Plaintiff downloaded one or more ostensibly "free" Apps from the App Store.

10. Plaintiffs can only use their iPhones in the confines of an environment controlled by Apple, as with other Apple "iDevice" products, such as the iPad.

11. All of Apple's iPhones consist of two inseparable components, namely the iDevice hardware and operating system firmware ("iOS"). As Apple has explained, "The iPhone firmware is not itself a product; it is a component of the iPhone mobile computing product."[1]

12. With much fanfare, Apple released its iPhone 3G in July 2008, which was purposely "designed to allow iPhone owners to safely and reliably download third party applica-

[1]Responsive Comment of Apple Inc., *In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Docket No. RM-2008-8 (U.S. Copyright Office), at 18 (Dec. 1, 2008) ("Responsive Comment").

tions."[2] Apple simultaneously launched its iPhone App Store to coincide with the release of the 3G iPhone.

13. Apple admits that since the launch of its iPhone 3G in 2008, the primary emphasis of its iPhone marketing campaigns is on the availability of 3rd party Apps the phones could run—not the ability of the mobile phone devices to make phone calls.[3]

14. Since Defendant Apple launched its mobile device business, it has maintained control over how the devices work, how consumers use them, and what happens when consumers use them—including functions Apple controls, hidden from consumers' sight, and used without consumers' consent. The downloadable Apps can only be created using Apple-supplied software development kits ("SDKs)," can only collect data from Plaintiffs' iPhones as permitted by Apple, and can only be distributed in Apple's captive-audience App Store upon Apple's approval.

15. Apple touts the privacy, confidentiality, and security of its Apple "ecosystem."

16. Apple induced the purchase of iPhones by Plaintiffs by offering thousands of ostensibly "free" Apps in its App Store. However, Apple failed to disclose to Plaintiffs that those "free" apps included third-party spyware[4] that utilized Apple-provided tools to collect Plaintiffs' information, without detection, and send it to third parties, like the Tracking Defendants.

17. For example, when Plaintiffs use Apps likes the Bible App, Dictionary.com App, Paper Toss App, and Urban Spoon App, those Apps routinely send information about Plaintiffs to Defendant Flurry, a third-party that amasses and analyzes such data. Flurry received Plaintiffs' device identifier information which it used to uniquely identify and track each Plaintiff, plus details such as what search terms they entered, which words they looked up in the dictionary, what version of the Bible they read, or even whether they shook the iPhone to allow the Urban Spoon app to choose a nearby restaurant—without ever providing Plaintiffs a

[2] See *id*. at 4-5.

[3] *Id*. at 6.

[4] The definition of "spyware" includes "any type of software that is surreptitiously installed on a computer and, without the consent of the user, could collect information from a computer . . . ." *FTC v. Pricewert*, Case. No. C-09-2407 (RMW) (N.D. Cal.), Order Appointing Temporary Receiver, June 15, 2009 (Dkt. 38).

clue that they were being watched, across their Apps, by the largest mobile analytics company in the world.

18. Worse yet, all the information transmitted through Plaintiffs' Apps to third parties was transmitted in an unreasonably insecure manner—contrary to accepted standards—and in a way that is well-recognized to be easily intercepted by even an unsophisticated hacker sitting near a wireless hotspot.

19. Plaintiffs have no means to avoid the data collection and tracking by Apple and the Tracking Defendants: Apple controls the ecosystem, Apple controls what Apps can and cannot transmit to third parties, and Apple controls the fact that its customers are kept in the dark about the spying built into its ecosystem.

20. Plaintiffs and similarly situated iPhone purchasers cannot learn about the spying that goes on except through unreasonably burdensome efforts, such as those required in the investigations underlying these allegations, which are by no means comprehensive.

21. Apple obtains revenue by marketing the ostensibly free Apps, and the availability of "free" Apps is tied to the availability of free data from spying on Plaintiffs and other iPhone purchasers, who had no idea what they are giving up, in terms of personal data, when they pay for an iPhone.

22. Plaintiffs did not consent to having their data collected by Apple and the third parties identified below.

23. Had Plaintiffs known of Defendants' practices within Apple's ecosystem, they would not have purchased iPhones or, certainly, would not have paid what they did for devices that are substantially devalued by such undesirable practices.

**B. Plaintiffs Continue to Pay For the GPS And Apps That Were Supposed to Be Free And Included In the Price of the iDevices.**

24. Apple freely admits that '[t]he iPhone Developer Program and the App store have played a significant part in the success of the 3G iPhone."[5]

25. Apple, however, fails to disclose adequately to Plaintiffs and Class Members the

[5] Responsive Comment, at 6.

fact that it created the App Store to furnish consumers' private and personally identifiable information, surreptitiously, to third-party advertising and analytics companies for their own collective commercial interests.

26. Plaintiffs here were induced to purchase the latest iPhone operating system and the App Store by the promise of access to a world of inexpensive, safe, and reliable Apps.

27. None of the Plaintiffs was informed by Apple or the Tracking Defendants that, to use "free" Apps or geolocation features on their iDevices, Plaintiffs would unknowingly provide data that would allow Defendants to personally identify them, and thereafter give Defendants full access to any user data on their iDevices as detailed below.

28. Each of the Plaintiffs purchased the iPhone believing the purchase included the advertised features provided by the host of "free" Apps available, unaware of the undisclosed costs that would be imposed on them by Defendants, including the appropriation of their iDevice resources and bandwith, as well the exploitation of their personal information.

29. Had Apple disclosed the true cost of the purportedly free Apps and geolocation features, the value of the iPhones would have been materially less than what Plaintiffs paid. Therefore, each of the Plaintiffs overpaid in the purchase of their iDevice.

**C. The GPS Functionality Advertised as an Included Feature of the iPhones Was Not Useable Without Apple Collecting Plaintiffs' Location Information, Even When Plaintiffs Selected the Option to Disable GPS.**

30. Apple intentionally designed its iOS 4 software to retrieve and transmit geolocation information located on its customers' iPhones to Apple's servers—even after customers, including Plaintiffs Gupta and Rodimer, explicitly denied Apple access to such data.

31. Apple expressly represented to consumers, including Plaintiffs Gupta and Rodimer, that they could prevent Apple from collecting geolocation data about them by switching the Location Services setting on their iPhones to "Off."

32. However, despite their explicit selections to the contrary, Apple continued to track and store information about Plaintiffs Gupta and Rodimer, and thousands of other consumers, even when Location Services was set to "off." As a result, Plaintiffs Gupta and Rodimer, and other similarly situated persons as defined below, could not prevent Apple from col-

lecting data about their location, even when they switched off the Location Services setting. Apple's representations to the contrary were false and/or misleading, and likely to deceive consumers targeted by such conduct.

33. Steve Jobs, Apple's founder and former CEO, put it most succinctly in a *Time* magazine interview in 2002: "Our job is to take responsibility for the complete user experience. And if it's not up to par, it's our fault, plain and simple."

34. Apple should not be permitted to now disclaim liability for the duties it so publicly undertook, but failed to fulfill, or for its own active role in facilitating and fostering an environment that encouraged routine violations of Plaintiffs' reasonable expectations and Apple's own public assurances.

## III. PARTIES

### A. Plaintiffs

35. Plaintiffs ("Plaintiffs") are United States residents who purchased mobile devices manufactured by Defendant Apple Inc. ("Apple"), that operate using Apple's proprietary operating system, iOS.

36. Plaintiff Jonathan Lalo, a resident of California, purchased an iPhone 3GS for $199 in or around June 2009; and iPhone 4 for $199 in June 2010, and an an iPhone 4S in or around October 2011.

37. Plaintiff Dustin Freeman, a resident of Arlington, Texas, purchased an iPhone 3GS from Apple in or around December 2009, and for which he paid $399.

38. Plaintiff Anthony Chiu, a resident of California, purchased an iPhone 4 in or around June 2010, for which he paid $299.

39. Plaintiff Daniel Rodimer, a resident of Florida, purchased an iPhone in or before March 2010 .

40. Plaintiff Jared Parsley, a resident of Royce City, Texas, purchased an iPhone 3G in or around August of 2008 and an iPhone 4 in or around October of 2010. His iPhone 4 was purchased from Apple and he paid approximately $399.

41. Plaintiff Heather Kimbrel, a resident of California, purchased an iPhone 4 in or

around August 2010, and for which she paid $250.

42. Plaintiff Kevin Burwick, a resident of California, purchased an iPhone 4 in or around June 2010, and for which he paid $200.

43. Plaintiff Marcia W. Burke, a resident of Alabama, purchased an iPhone in or around December 2007, and for which she paid $200.

44. Plaintiff William C. Burke III, a resident of Alabama, originally purchased an iPhone in or around December 2007, which he traded in for an upgraded iPhone in or around December 2010.

45. As to each and every Plaintiff named above:

a. They downloaded and used numerous free Apps from the App Store during the Class Period, as detailed below in paragraphs 58 through 68, and each was subjected to the collection of personal information and information about their iDevices by Tracking Defendants.

b. At no time did any of the above-named Plaintiffs ever authorize Apple or any App to cause such information to be shared with any third-party advertising network or analytics provider, or be used for third party advertising purposes.

c. Each Plaintiff named above considered his or her personal information to be private property and/or a confidential asset that has an ascribed economic value to Plaintiff.

46. Plaintiff Arun Gupta, a resident of Georgia, purchased an iPhone 4G in or around December 2010.

a. Mr. Gupta had set the Location Services function on his iPhone to "off," yet data revealing his geolocation was collected and transmitted to Apple's servers without his authorization.

b. At no time did Plaintiff Gupta ever authorize Apple, any App, or any advertising network to track his geolocation.

c. Plaintiff Gupta considers his personal information to be his private property, and he ascribes economic value to it.

47. Similarly, Plaintiff Rodimer had set the Location Services function on his iPh-

one to "off" and at no time did he authorize Apple, any App, or any advertising network to track his geolocation. Yet, data revealing his geolocation was collected and transmitted to Apple's servers without his authorization.

**B. Defendant Apple**

48. Defendant Apple Inc. ("Apple") is a California corporation with its principal place of business at 1 Infinite Loop, Cupertino, California 95014.

49. Apple is the maker of the Apple iPhone and the developer of iOS, the operating system that runs those devices.

50. Apple developed and operates the Apple App Store.

51. Apple reviews and approves each and every App that it offers in the App Store.

**C. Tracking Defendants**

52. The Defendants named below, collectively referred to in this complaint as the "Tracking Defendants," collect personal information transmitted from Plainitffs' iDevices for purposes unrelated to the functionality of Plaintiffs' iDevices or execution of Apps on those devices.

53. Defendant Flurry, Inc. ("Flurry") is a Delaware corporation with its principal place of business in San Francisco, California. Flurry is an advertising content and analytics provider for mobile device applications. Specifically, Flurry assists App developers by providing "demographic, geographic and user interest data." Flurry explains that "[w]hile having age and gender is powerful, once you add geography to the mix, you have the trifecta for how any audience is described… Flurry Analytics gives you all three, automatically." In addition, Flurry touts that "Flurry shows you what other apps your consumers use…."

54. Defendant AdMarvel, Inc. ("AdMarvel") is a Delaware corporation with its principal place of business in San Mateo, California. AdMarvel is a mobile advertising provider that partners with other advertising networks to provide mobile advertising content to mobile devices. AdMarvel schedules, serves and tracks ad units, and states that it enables clients to "track and monetize [their] mobile audience," and purports to be able to target handsets, campaigns, and operating systems, and leverage demographics, page content and keywords.

55. Defendant Google, Inc. is a company organized and existing under the laws of the State of Delaware, with its principal place of business located in San Mateo, California. Google, Inc. operates ad network DoubleClick, and provides analytics services through Google Analytics.

56. Defendant AdMob, Inc. ("AdMob") is a company organized and existing under the laws of the State of Delaware, with its principal place of business at 1600 Amphitheatre Parkway, Suite 225, Mountain View, CA 94043. AdMob, which was acquired by Google, Inc. in 2009, purports to be "the world's largest mobile advertising marketplace" offering "both advertisers and publishers the ability to target and personalize advertising to their customers in 150 countries." Admob offers "sophisticated targeting options [which] include demographics, interests and behavioral, device and carrier, keyword and remarketing." In particular, AdMob accesses the GPS location, application package name, and application version information off of iDevices. Additionally for some Apps, it appears that AdMob transmits Plaintiffs and Class Members' birthday, gender, and postal code information, from which it has been demonstrated there is an extremely high probability the unique user of the device can be determined.

57. Defendant Medialets, Inc. ("Medialets"), is a Delaware corporation with its principal place of business at 450 West 15th Street, Suite 200, New York, New York 10011. Medialets is a provider of analytics services for mobile devices, .

58. Regarding third-party data analytics company, **Flurry**:

a. Through the Bible App, Flurry collected from Plaintiff Rodimer information about which version of the Bible Plaintiff selected from the over 150 versions of the Bible available in the App (*e.g.*, *King James Version*, *New American Bible*, *New International Version*, *etc.*).

b. Flurry's collection of Bible version information in the Bible App constituted the collection of information related to religious practices, not only because of the nature of the App, itself, but also because certain versions of the Bible available through the App tend to be associated with particular institutions, such as the Roman Catholic Church or evangelical Protestant denominations, or particular religious beliefs and affiliations, such as versions asso-

ciated with conservative or liberal language or doctrine. Bible version information also relates to personal characteristics, such as versions designed for children or translations in various languages.

c. Through Dictionary.com App, Flurry repeatedly collected the following from Plaintiffs Chiu and Lalo during their use of the App: which words Plaintiffs looked up; the titles of particular pages in the App Plaintiffs viewed; and the particular App activities Plaintiffs used (*e.g.*, search, view, Word of the Day).

d. Through the Urban Spoon App, for locating area restaurants, Flurry collected from Plaintiff Chiu the titles of particular App pages he viewed, the particular App activities in which he engaged (*e.g.,* search, view), including whether he shook his iPhone to activate Urban Spoon's restaurant-suggestion function.

e. Each time Flurry collected the information from Plaintiffs as they used the above-indicated Apps, Flurry also collected the additional information from each of Plaintiffs' iDevices including, but not limited to: UDID; device type (*e.g.*, "iPhone," "iPad") and model; name of the device's operating system and operating system version; Plaintiff's time zone; and language.[6] .

59. Regarding third-party mobile ad network, **AdMarvel**:

a. Through the Dictionary.com App, AdMarvel repeatedly collected the following information from Plaintiffs Chiu and Lalo, with each use of the app: UDID; network type (*e.g.*, 3G or WiFi); and the name of the device's operating system and operating system version. In addition, AdMarvel collected Plaintiffs' carrier-assigned user names (*e.g.*, "JOHN'S PHONE").

b. The Pandora app, which allows a user to receive streamed, customized music selections, was installed and used by Plaintiffs Burwick, Chiu, Freeman, Kimbrell, Lalo, Parsley, William C. Burke III, and Marcia W. Burke. Admarvel tracked each of the Plaintiffs

[6] Reportedly, Apple has limited the availability of some device data in its iOS version 5. Even if so, millions of iPhone purchasers continue to use the prior version.

using a unique identifier—not the iDevice UDID—but an identifier AdMarvel downloaded from DoubleClick, an unaffiliated third-party ad network owned by Google.

c. In addition, the Pandora App included code causing the unaffiliated third-party ad network, AdMarvel, to be contacted and sent information regarding Plaintiffs that included: date of birth, gender, income, education level, and partners sought.

60. Regarding third-party ad network, **DoubleClick**:

a. Through the Pandora App, DoubleClick collected the following information from Plaintiffs Burwick, Chiu, Freeman, Kimbrell, Lalo, Parsley, William C. Burke III, and Marcia W. Burke: age, gender, zip code, particular song and performer selected, and music genre, all linked to the unique identifier that DoubleClick shares with AdMarvel, discussed above in paragraphs 59(b) and (c).

b. Through the Flixster App, DoubleClick collected the following information from Plaintiff Chiu: an identifier for the particular movie for which Plaintiff requested information, genre, movie rating, and whether a "Certified Fresh" review was available from Flixster's Rotten Tomatoes website.

c. In addition, through the Flixster App, DoubleClick collected Plaintiff Chiu's information regarding type of device operating system; whether or not an SD memory (data storage) card was installed on Plaintiff's iPhone; whether the iPhone was jail-broken (modified by users); and keywords for other data values.

d. Through the Weather Channel App, DoubleClick collected the following information from Plaintiffs Burwick, Freeman, Kimbrell, and Lalo: Plaintiff's zip code and iDevice model (*e.g.*, iPhone 4G).

e. Through the Urban Spoon restaurant search App, DoubleClick collected the following information from Plaintiff Chiu: UDID and fine (GPS-based) location information. In addition, the App sent the following information about Plaintiff's use of the app: type of search and food type.

61. Regarding third-party mobile ad network, **AdMob**, also owned by Google, the Bible App, used by Plaintiff Rodimer, sent AdMob the App Store identifier for the Bible App (282935706).

62. Regarding third-party analytics company, **Google Analytics**:

a. Through the Bible App, Google Analytics collected the identifier for the Bible version selected by Plaintiff Rodimer.

b. Through the Dictionary.com App, Google Analytics collected the search terms entered by Plaintiffs Chiu and Lalo.

c. Through the Flixster App, Google Analytics collected the following information from Plaintiff Chiu: the particular movie for which Plaintiff requested information, Plaintiff's activity within the app, and pages (including movie information and theater information pages) viewed by Plaintiff; and the name of the iDevice's operating system and operating system version.

63. Regarding third-party mobile analytics provider, **Medialets**:

a. Through the Weather Channel App, Medialets collected the following information from Plaintiffs Burwick, Freeman, Kimbrell, and Lalo: UDID; the name of the device's operating system; and iDevice model (*e.g.*, iPhone 4G), and app name.

b. In addition, Medialets downloaded to each Plaintiffs' iDevices a 1-2 megabyte zip archive with which Medialets created an advertising-related SQLite database in Plainitffs iDevice's data storage area, consuming bandwidth resources for the download process and, subsequently, device storage resources.

64. In summary, of the above-mentioned apps downloaded and used by Plaintiffs, the information collected from each Plaintiff and transmitted to third parties included:

a. From Plaintiff Burwick: fine (GPS) location information, network (*e.g.*, 3G or WiFi), name of the device's operating system, operating system version, the amount of free storage space on iDevice, the carrier-assigned phone name (*e.g.*, "Jim's phone"), iDevice model (*e.g.*, iPhone 3GS), and the phone's unique device identifier (UDID), Plaintiff's age, Plaintiff's gender, Plaintiff's app ID and password for specific App accounts, the search term

entered by Plaintiff, time zone, language, Plaintiff's zip code, the name of the app, the title of particular app page viewed by Plaintiff, the particular app activity engaged by Plaintiff (e.g., search, view), Plaintiff's particular media selection (e.g., song, video), the genre of media selected by Plaintiff, and the performer in Plaintiff's media selection.

b. From Plaintiff Chiu: fine (GPS) location information, network (e.g., 3G or WiFi), name of the device's operating system, operating system version, the amount of free storage space on iDevice, the carrier-assigned phone name (e.g., "Jim's phone"), and the phone's unique device identifier (UDID), Plaintiff's age, Plaintiff's gender, Plaintiff's app ID and password for specific App accounts, the search term entered by Plaintiff, time zone, language, Plaintiff's zip code, the name of the app, the title of particular app page viewed by Plaintiff, the particular app activity engaged by Plaintiff (*e.g.*, search, view), Plaintiff's particular media selection (*e.g.*, song, video), the genre of media selected by Plaintiff, and the performer in Plaintiff's media selection.

c. From Plaintiff Freeman: fine (GPS) location information, name of the device's operating system, operating system version, iDevice model (e.g., iPhone 3GS), and the phone's unique device identifier (UDID), Plaintiff's age, Plaintiff's gender, Plaintiff's app ID and password for specific App accounts, Plaintiff's zip code, the name of the app, the title of particular app page viewed by Plaintiff, the particular app activity engaged by Plaintiff (e.g., search, view), Plaintiff's particular media selection (e.g., song, video), the genre of media selected by Plaintiff, and the performer in Plaintiff's media selection.

d. From Plaintiff Kimbrell: fine (GPS) location information, name of the device's operating system, operating system version, iDevice model (e.g., iPhone 3GS), and the phone's unique device identifier (UDID), Plaintiff's age, Plaintiff's gender, Plaintiff's app ID and password for specific App accounts, Plaintiff's zip code, the title of particular app page viewed by Plaintiff, the particular app activity engaged by Plaintiff (e.g., search, view), Plaintiff's particular media selection (e.g., song, video), the genre of media selected by Plaintiff, and the performer in Plaintiff's media selection.

e. From Plaintiff Lalo: fine (GPS) location information, network (e.g., 3G

or WiFi), name of the device's operating system, operating system version, the carrier-assigned phone name (e.g., "Jim's phone"), iDevice model (e.g., iPhone 3GS), and the phone's unique device identifier (UDID), Plaintiff's age, Plaintiff's gender, the search term entered by Plaintiff, time zone, language, Plaintiff's zip code, the name of the app, the title of particular app page viewed by Plaintiff, the particular app activity engaged by Plaintiff (e.g., search, view), Plaintiff's particular media selection (e.g., song, video), the genre of media selected by Plaintiff, and the performer in Plaintiff's media selection.

f. From Plaintiff Parsley: name of the device's operating system, operating system version, Plaintiff's age, Plaintiff's gender, Plaintiff's app ID and password for specific App accounts, Plaintiff's zip code, Plaintiff's particular media selection (e.g., song, video), the genre of media selected by Plaintiff, and the performer in Plaintiff's media selection.

g. From Plaintiff Rodimer: name of the device's operating system, operating system version, and the phone's unique device identifier (UDID), time zone, language, the name of the app, the title of particular app page viewed by Plaintiff,

65. In addition to the personal information transmitted to third parties, Plaintiffs' Apps were able to access and transmit Plaintiffs' personal information to the Apps, themselves, including information such as: fine (GPS) location information, network (*e.g.*, 3G or WiFi), name of the device's operating system, operating system version, the amount of free storage space on iDevice, and the phone's unique device identifier (UDID), Plaintiff's app ID and password for specific App accounts, the search term entered by Plaintiff, the title of particular app page viewed by Plaintiff, and the particular app activity engaged by Plaintiff (e.g., search, view).

66. Not only was Plaintiffs' personal information transmitted to the above-named third parties and to the Apps, themselves, but all of Plaintiffs' information listed above was transmitted "in the clear" (sometimes referred to as "plain text"), that is, without encryption.

67. Such transmission in the clear was substandard in light of reasonably accepted security measures, exposing each Plaintiff to unreasonable risks of the interception of their personal information that are well understood to be associated with such poorly secured transmis-

sion.[7]

68. Such unsecured transmissions were particularly inappropriate given the nature of mobile devices and Apps through which such information was transmitted, because of the likelihood of using mobile devices and such Apps in mobile hot-spots, which often employ no security settings to protect wireless communications,[8] and because of the likelihood that many users of such Apps are minors.

## IV. JURISDICTION AND VENUE

69. This Court has subject-matter jurisdiction over this action pursuant to:

a. Title 28, United States Code, Section 1331; and

b. The Class Action Fairness Act of 2005, 28 U.S.C. Sections 1332(a) and (d), because the amount in controversy exceeds $5,000,000.00 exclusive of interest and costs, and more than two thirds of the members of the Class are citizens of states different from those of Defendants.

70. Under CAFA, the federal courts have exclusive jurisdiction over all actions with an amount in controversy in excess of $5,000,000. Here, the statutory claims alone have a value far in excess of that amount, which establishes jurisdiction.

71. Venue is proper in this District under Title 28, United States Code, Section 1391(b) because Defendants' improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district. Five of the defendants are California corporations with their principal places of business in this district.

72. Each of the Plaintiffs has standing to bring this case under Article III of the United States Constitution as follows:

a. Plaintiffs have standing by virtue of alleging concrete, tangible and non-

[7] According to the National Institute for Standards and Technology (NIST), "Mobile devices have a broad attack surface including Bluetooth, Wi-Fi, and cellular communications interfaces as well as protocols for Web transactions," and "[s]ensitive data should be encrypted during data transmission and when stored on the device or in external memory cards." Wayne Jansen, Karen Scarfone, *Recommendations of the National Institute of Standards and Technology: Guidelines on Cell Phone and PDA Security*, U.S. Dept. of Commerce, NIST, SP 800-124 at 3-2 (Oct. 2008).

[8] See "US-CERT Cyber Security Tip ST05-003 – Securing Wireless Networks" at http://www.us-cert.gov/cas/tips/ST05-003.html.

speculative injuries in fact, arising from violations of Federal statutes and the California Constitution. The statutes and Constitutional provisions at issue herein create legal rights, the invasion of which creates standing;

b. Plaintiffs and the Class members are within the zone of persons sought to be protected by these statutory and Constitutional provisions, and if Plaintiffs cannot protect such interests and seek either remuneration or injunctive relief, they would have no mechanism available to hold Defendants accountable for such misconduct;

c. Plaintiffs have each suffered harm and economic injury as a result of each Defendants' actions which have caused Plaintiffs to pay more for their iDevices than they otherwise would have;

d. Plaintiffs have each suffered harm and economic injury as a result of each Tracking Defendant surreptitiously including in App software certain code components that Plaintiffs would not reasonably have expected to be included, and which was installed, along with the expected software, on their devices without their permission, and which consumed portions of the "cache" and/or gigabytes of memory on their devices—memory that Plaintiffs paid for the exclusive use of when they purchased their iDevices;

e. Plaintiffs' personal data is property[9] that was obtained by third parties that Plaintiffs did not know, and who did not have Plaintiffs' permission to access such data in the absence of Plaintiffs' and Class members' knowledge or consent. Plaintiffs' personal property data and/or personal data assets include but are not limited to UDID information, demographic information, geolocation information, and application usage habits;

f. Plaintiffs have each suffered harm and economic injury as a result of each Defendants' conduct which has imposed undisclosed data transmittal costs on Plaintiffs;

g. Defendants' conduct caused harm to the value and security of Plaintiffs'

[9] *See* P. Schwartz; Property, Privacy and Personal Data, 177 Harvard L. Rev. 2005 (2004) (describing four hallmarks to property in the form of personal data: (1) it is inalienable in that consumers have a right to say who does and who does not have access to such information and can limit its transferability, ownership or use; (2) the right to opt in or opt out of the sharing or use of such information; (3) the right to exit out of any data trading processes once that initial selection is made; and (4) a quantifiable loss attributable to the unauthorized access to such data or using it beyond the consent provided by consumers).

personal, and personally identifiable, information;

h. Defendants' conduct caused harm in that they individually violated Plaintiffs' legally protected privacy right to seclusion in their affairs by, in the aggregate, collecting Plaintiffs' personal information, to de-anonymize Plaintiffs and to personally identify them, and their activity;

i. The data collected from Plaintiffs and Class Members are raw material that has an independent, objective market value to both Plaintiffs and Defendants. It is separate and unique to each Plaintiff, respectively;

j. Plaintiffs and members of the Class suffered damage and were injured in fact by having lost control of their personal data assets;

k. Defendants have placed an independent value on such data by paying market-set prices to access Plaintiffs' data;

l. Plaintiffs lost and have not been compensated for the value of such data, and, Defendants have infringed the inherent property right to control such data;

m. Plaintiffs possess an ownership interest in their data that belongs to them and is subject to their control and alienability, and is a valuable commodity that has a property market value to advertisers. Plaintiffs thus have had property, with an independent value taken from them, by it passing beyond their control, without compensation;

n. As such information was taken without their full knowledge or consent, and without Plaintiffs having obtained any compensation for the raw material taken from them, such a loss constitutes a classic Article III injury in terms of an uncompensated loss for which this Court can provide redress;

o. These data also have an independent, quantifiable economic value to Plaintiffs. According to a peer-reviewed study published in the May 2007 edition of the Journal of Management Information Systems, U.S. consumers who were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use -- the two concerns at issue here -- valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between

$7.98 and $11.68 per website. This is consistent with the Plaintiffs' valuation of their own data.

73. As with any form of property, Plaintiffs, as the owners, should be compensated for the use and exploitation thereof, and if they are not, they suffer concrete, measurable damage and injury, the exact amount of which shall be provided by Plaintiffs through expert opinion.

## V. GENERAL ALLEGATIONS

### A. The Sale and Use of iDevices

74. Apple manufactures, licenses, distributes, and promotes iDevices, including the iPhone, throughout the country, including in the State of California.

75. Apple materially misrepresented the true cost of the iDevices and/or omitted material information from its representations.

76. Plaintiffs and Class Members relied upon Apple's representations with respect to the cost of their iDevices, the availability of "free" Apps, and the ability to opt-out of geolocation tracking, in making their purchasing decisions, and the omission of material facts to the contrary was an important factor to them.

77. Apple has represented to Plaintiffs and consumers, expressly or by implication, that the App Store does not permit apps that "violate[] our developer guidelines" including apps containing pornography, apps that violate a users privacy, and apps that hog bandwidth.

78. Apple has represented to Plaintiffs and consumers, expressly or by implication, that: "Apple takes precautions — including administrative, technical, and physical measures — to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction."

79. Plaintiffs were not informed as to the true cost of their iDevices due the lack of disclosures about third party tracking, tracking by Apple (even when Location Services were set to Off) and the data transmittal and storage costs that would be imposed, and the iDevice resources that the Defendants would secretly consume.

80. Plaintiffs and Class Members would not have purchased their iDevices and/or would not have paid as much for them, if Apple had disclosed the true facts that it and the

Tracking Defendants would surreptitiously obtain personal information from their iDevices, track their activity and geolocation, and consume portions of the "cache" and/or gigabytes of memory on their devices—memory that Plaintiffs paid for the exclusive use of when they purchased their iDevice.

81. Because Apple did not disclose the true costs of their iDevices, Plaintiffs were misled into purchasing a product that did not meet their reasonable expectations.

82. Given the undisclosed costs imposed by using the iDevice, it was not as valuable to Plaintiffs as the price they paid for it.

83. Apple's competitors manufacture, market, and distribute comparable mobile devices that do not collect personal information and track Plaintiffs without permission, or adequately disclose those material facts.

84. Plaintiffs and Class Members paid a premium for their iDevice, in part because of Apple's material misrepresentations and omissions about the availability of a large number of "free" Apps that were not actually free as Plaintiffs reasonably believed.

85. "Since the introduction of the App Store, overall consumer response to the iPhone itself increased dramatically."[10] While it took 74 days for Apple to sell one million units of its 1st generation iPhone, consumers purchased one million App-ready 3G iPhones in just 3 days.

86. The Apple App Store was a market differentiator that not only set Apple iPhones apart from its handset competitors, it set the newly released iPhone 3G, with its 2.0 iOS operating system, apart from the prior generations of iPhones. In the post 3G 2.0 iOS era, the success of Apple's iPhones sales is inextricably linked to consumers' access to its App Store.

87. Plaintiffs and Class Members suffered actual damages as a result of Apple's acts and omissions. Specifically, as a proximate result of Apple's conduct, Plaintiffs and other Class Members suffered monetary losses, i.e., the purchase price of the iDevice, or at a minimum, the

[10] Responsive Comment, at 5.

difference of the inflated price and the price Apple should have charged for a product that fully disclosed all the costs hidden by Apple.

88. iDevices and Apps are now used by many consumers in almost all facets of their daily lives. Among others, there are Apps for business use, such as contact management and business expense tracking, for personal finance use, such as trading and banking;, as well as for media, news outlets, education (such as childbirth education and children's math learning); and entertainment, such as movie reviews and electronic games.

89. Every App in the App Store, whether free or paid, must be approved by Apple and digitally signed by Apple. Both Apple and third-party developers create numerous Apps available from the App Store. There are several hundred thousand Apps available at the App Store.

90. Apple also offers other Apps through its App Store that are developed by Apple, some of which are free to consumers and some of which are sold.

91. Apple has complete discretion as to whether it will allow an App to be sold in the App Store.

92. Apple requires that proposed Apps go through a rigorous approval process. Even if an App meets the "Program" requirements (as Apple describes it), Apple may still reject the App for any reason at all. It is estimated that approximately 20 percent of all third-party requests to place Apps for sale in the App Store are rejected by Apple.

93. iDevice users are only allowed to download software specifically licensed by Apple and available on the iDevice out of the box or through the App Store.

94. If a user installs any software not approved by Apple, the users' warranty is voided. When a user installs Apple's updates to the iDevice operating system, Apple takes the opportunity to erase any non-licensed software on the device. Apple claims this control is necessary to ensure the "tightly integrated," smooth functioning of the iDevice.

95. Even after a user downloads an approved app, Apple maintains control by requiring that the end-user license agreement for every App include a clause giving Apple the ability to step into the shoes of the App developer and sue the end-user. If Apple is a third party

beneficiary of that contract, then Plaintiffs are third party beneficiaries of any contract between the App developer and Apple that requires the protection of, and restricts access to, personal consumer information contained on the iDevice. Specifically, the iOS Developer Agreement states:

> **9. Third Party Beneficiary:** You and the end-user must acknowledge and agree that Apple, and Apple's subsidiaries, are third party beneficiaries of the EULA, and that, upon the end-user's acceptance of the terms and conditions of the EULA, Apple will have the right (and will be deemed to have accepted the right) to enforce the EULA against the end-user as a third party beneficiary thereof.

**B. Apple Controls the Development Process for Apps Available for iDevices**

96. In addition to controlling the characteristics and distribution of Apps, described above, Apple exercises substantial control over their development and functionality.

97. A third party who wants to sell an App from the Apple App Store is required to pay to enroll in the iPhone Developer Program.

98. The third party must also agree to the terms of Apple's iPhone Developer Program License Agreement ("iOS Developer Agreement"). The iOS Developer Agreement is, by its terms, confidential, and prohibits the third party from making any public statements about the agreement, its terms and conditions, or the third party's relationship with Apple without Apple's prior written approval.

99. The third party must create the App using Apple's Software Development Kit software (SDK), which can only be installed on an Apple computer. An App developed using Apple's SDK will only function on iDevices and can only interact with the iDevice operating system and features in the ways permitted by the iOS Developer Agreement and SDK.

**(1) Apple Uses Plaintiffs' Personal Information to Lure Low Cost Apps to its App Store.**

100. Apple's relationship with its App developers is also clearly symbiotic—Apple needs to have a healthy stable of low cost or free Apps available in its App Store to satisfy customer demands for the ability to customize their iDevices.

101. Apple takes steps to satisfy App developers' monetary requirements in order to

encourage App developers to continue to provide a steady stream of low cost or free Apps for distribution in the App Store. The primary way Apple has done so is by ensuring that App developers have maintained access to a steady supply of valuable information about Plaintiffs. The App developers then use that information about Plaintiffs to obtain advertising revenue from the Tracking Defendants.

102. One of the most valuable pieces of information that the Tracking Defendants obtain is access to Plaintiffs' Apple-assigned UDID information. Apple knows the Tracking Defendants obtain and use the UDID from Plainitffs' iDevices, and Apple has failed to end that practice or meaningfully enforce any policy against it.

103. Apple understands the significance of identifiers such as its UDID in regards to users' privacy. Indeed, internally, Apple claims that it treats UDID information as "personally identifiable information" because, if combined with other information, such as other information easily available on the iDevice, it can be used to personally identify a user. This is due to the *globally* unique nature of a UDID—no other device bears the same identifying number.

104. That is exactly what happened with each Plaintiff in this litigation, as well as with all of the members of proposed iDevice Class -- Plaintiffs UDID information, along with other data like geographic location data, was collected by each Tracking Defendant, such that each Tracking Defendant was able to personally identify each Plaintiff. Once this was accomplished, every other piece of information collected by the Tracking Defendants was tied to Plaintiffs' respective identities and used to further build a more complete profile of Plaintiffs.

105. Because Plaintiffs' UDID is unique to each iPhone, and because each Plaintiff is the only, or at least the primary, user of their iDevice, the UDID proved to be an invaluable feature for the Tracking Defendants who were looking for a means of reliably identifying and tracking Plaintiffs' online activities.

106. It was completely foreseeable to Apple that this would occur and, in fact, was to Apple's direct benefit. Apple knowingly and intentionally allowed the Tracking Defendants to access Plaintiffs' iDevices' UDID and chose to not provide Plaintiffs with any means to disable the iDevice's UDID from being tracked or to restrict access to the UDID.

107. Apple's desire to encourage and incentivize App developers is also evidenced by Apple allowing the Tracking Defendants to have access to numerous other pieces of information that Plaintiffs consider personal. For example: Apple allows App developers to build Apps that—by design by Apple—will easily access the following personally identifiable information on a consumer's iDevice:

a. *geolocation*: in the */Library/Application Support/MobileSync/Backups/* folder on a user's iDevice, Apple maintains an unencrypted log of the user's movements, as often as 100 times a day, for up to a one-year period; Apple logs a user's geolocations even if the user has disabled the iDevice's Location Services GPS features, apparently by using cell transmitter tower signals to triangulate the user's location; Apple replicates this file on any computer with which the user synchs an iDevice;

b. the numerous items of information collected from Plaintiffs and their iDevices, as set forth in section III. C, "Tracking Defendants," above.

108. Because of the items of personally identifiable information transmitted from each Plaintiff, even otherwise non-identifiable information, once associated with identity, itself is considered personally identifiable information.

109. Apple allowed third parties access to that information even as it specifically represented to Plaintiffs that it did not allow Apps that violate Plaintiffs' privacy.

110. Apple appeared to recognize the conflicted nature of its approach, as, in April of 2010, Apple amended its Developer Agreement, purportedly to ban Apps from sending data to third parties, except for information directly necessary for the functionality of the App. Apple's revised Developer Agreement provided that "the use of third party software in Your Application to collect and send Device Data to a third party for processing or analysis is expressly prohibited."

111. Apple faced a mountain of criticism over this change, so in September 2010, it amended its Developer Agreement again to allow for a significant exception—to allow transmission of data for advertising purposes (but not for data compilation and analytics purposes).

112. These changes were not engendered by a concern over consumers' data, howev-

er, but only by a concern for protection of Apple's own device data. Ironically, Apple discovered that third party analytics companies such as Flurry were able to obtain device data about unreleased Apple prototypes (that were used for internal purposes on the Apple campus), because such data was being transmitted via Apps that Apple had installed on the devices. Neither of Apple's amendments to its Developer Agreements directly addressed use of UDID data.

113. After the filing of this lawsuit, however, Apple quietly changed its policy regarding third-party access to UDID information. With the introduction of its iOS 5 operating system, Apple appears to have taken steps to finally stop Apps from sharing UDID information, but not before Plaintiffs and members of the class were significantly harmed. Apple has not offered a clear explanation for this change and the Tracking Defendants, starved of a critical piece of data necessary to identify and track Plaintiffs, are already seeking alternatives to the UDID.

114. Another example of Apple allowing Apps access to iDevice users' information involves Apple collecting users' location information in an easily accessible database file on the users' iDevice, and any other Apple device used to synchronize or back-up the iDevice.

115. In June 2010, with the release of its iOS 4 operating system, Apple began intentionally collecting Plaintiffs' precise geographic location (consisting of accurate longitude and latitude coordinates) and storing that information in a file on the iDevice called "consolidated.db." These files accumulated a log of the longitude and latitude for every place Plaintiffs traveled, along with a timestamp. The geographic location information was pulled either from Wi-fi towers or cell phone towers in Plaintiffs' vicinity, and in some cases from the GPS data on Plaintiffs' own iDevices.

116. In essence, this file constitutes a timeline and map of Plaintiffs' every move. This data was also transmitted to Apple, and unknowingly uploaded by Plaintiffs every time they synchronized ("synced") their iDevice to their home computer or another Apple device. The file data was, unbeknownst to Plaintiffs, also available through Apps to third party marketers.

117. As Apple explains in its patent application for the iOS 4 operating system (U.S.

Patent Application Number 20110051665"): "The location history can be used to construct a travel timeline for the location aware device. The travel timeline can be displayed in a map view or used by location aware applications running on the location aware device or on a network. In some implementations, an Application Programming Interface (API) can be used by an application to query the location history database."

118. The data files at issue constitute a significant amount of solid-state memory space on Plaintiffs' iDevices. Although the file size varies among Plaintiffs, the Plaintiffs believe that the range of sizes for such files for each class member is between 10 and 40 megabytes (which is enough space to store dozens of songs or photographs).

119. Based on the premium that Apple charges for its iDevices with extra solid-state memory space (*i.e.,* 32 gigabyte models rather than 16 gigabyte models) the memory space on iDevices has a reasonable market value of $100 per 16 gigabytes.

120. Based on this number, the amount of solid-state memory space consumed by Apple for the undisclosed geolocation file is equal to approximately twenty-three cents ($0.23), for each Plaintiff's iPhone.

121. The storage space on Plaintiffs' iDevices is storage space they paid for, and the twenty-three cents worth of storage that Apple consumes on Plaintiffs' and class members' iDevices for Apple's own purposes constitutes a taking of an asset of economic value, paid for by Plaintiffs and Class Members and to which they have a superior right of possession. Apple's use of this space renders it unavailable for use by the owners of the iDevices.

122. Apple does not adequately disclose its practices regarding the geolocation tracking and the iDevice resources it consumes. Plaintiffs paid Apple for these solid-state memory e resources, yet Apple essentially took it back from Plaintiffs without their permission, consent or knowledge.

**C. Apple Failed To Protect User Privacy and the Security of User Data as Promised**

123. As discussed above, Apple's control of the user experience includes restrictions, such as blocking consumers from modifying devices or installing non-App-store Apps, and blocking developers and researchers from publicly discussing Apple's standards for App de-

velopment, and even prohibiting researchers from analyzing and publicly discussing device shortcomings such as privacy flaws.

124. As a direct consequence of the control exercised by Apple, Plaintiffs and Class Members Class could not and cannot reasonably review the privacy effects of Apps and must rely on Apple to fulfill its duty to do so.

125. Apple undertook a duty to Plaintiffs and consumers to protect their privacy, representing that it reviews all Apps available in its App Store for suitability, and that it retains broad discretion to remove an App from the App Store.

126. A third party cannot upload an App for sale in the App Store until Apple digitally signs the App, thereby signifying Apple's review and approval of the App for sale in the App store.

127. Apple represents that an App may not access information from or about the user stored on the user's iDevice unless the information is necessary for the advertised functioning of the App.

128. Apple represents that it does not allow one App to access data stored by another App.

129. Apple represents that it does not allow an App to transmit data from a user's iDevice to other parties without the user's consent.

130. Despite its representations and the duties to Plaintiffs and Class Members Apple undertook to protect their personal information from being accessed and exploited by third parties like the Tracking Defendants, Apple knowingly permits Apps that subject consumers to privacy exploits and security vulnerabilities to be offered in the App Store.

131. Contrary to Apple's representations to Plaintiffs and consumers, Apple does not screen App Store candidates to determine their use of proper standards in transmitting personal information or analyze the traffic generated by Apps to detect Apps that violate the privacy terms of the iOS Developer Agreement and Apple's commitments to users.

132. Apple has a duty of reasonable care that arises independent of its promises and its undertaken duties. Apple shares the duty everyone shares to use ordinary care to prevent

others from being injured as the result of its conduct. This duty arises independently of any contractual provision.

133. Apple also has a special relationship with Plaintiffs, its customers, that placed a duty of reasonable care to act in a reasonable manner in designing its product so as to prevent Plaintiffs from being harmed; to warn Plaintiffs of any harm of which it is aware might foreseeably occur; or take reasonable steps to prevent others from causing Plaintiffs harm when that harm is reasonably foreseeable by Apple.

134. Apple breached each of these duties to Plaintiffs in failing to act with reasonable care as outlined in the preceding sections.

135. Apple's breach of its duties caused foreseeable harm to Plaintiffs and was a proximate cause thereof, as outlined in the preceding sections.

**D. Apple's Collection of Geolocation Data**

136. "You may not know it, but if you carry a smartphone in your pocket, you are probably doing unpaid work for Apple… and helping [it] eventually aim more advertising directly at you."[11]

137. Apple is developing an expansive database containing information about the geographic location of cellular towers and wireless networks throughout the United States. This information forms the underlying data necessary for a digital marketing grid that Apple can use to accurately deploy targeted advertisements to mobile phone users in the future. A digital marketing grid of this scope is highly lucrative to Apple, as the mobile phone advertising industry is projected to become a $2.5 billion dollar market by 2015.

138. In order to collect the information needed to create the digital marketing grid described above, Apple designed its iPhone's iOS 4 to collect and send geolocation data retrieved from its customers' iPhones to Apple's servers, including, *inter alia*, information revealing the unique identifiers of nearby cellular towers and wireless networks.

11 Apple and Google Use Location Data to Map the World, http://www.nytimes.com/2011/04/26/technology/26locate.html (last visited October 21, 2011).

**E. Apple Misled Plaintiffs About Opting-Out Of Its Tracking Program**

139. Apple's Terms and Conditions ("TAC") expressly stated that customers could opt-out of Apple's tracking program and prevent geolocation information from being collected and sent from their iPhones:

> Location Data: Apple ... may provide certain services through your iPhone that rely upon location information. To provide these services, where available, Apple ... may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone ... By using any location-based services on your iPhone, you agree and consent to Apple's ... transmission, collection, maintenance, processing and use of your location data to provide such products and services. *You may withdraw consent at any time by ... turning off the Location Services setting on your iPhone*[.]

(Terms and Conditions, ¶ 4(b)) (emphasis added.)

140. Similarly, in a letter to Congress, Apple stood by its purported opt-out procedure, and expressly represented that if customers turn "Off" the location-based services settings on their iPhone, then "no location-based information will be collected or transmitted."[12]

141. Unfortunately, despite the fact that many iPhone users, including Plaintiffs Gupta and Rodimer, affirmatively withdrew their consent to be tracked by turning off their iPhones' Location Services, Apple still continued to collect and transmit geolocation information.

142. Despite Apple's statements to the contrary, Apple designed iOS 4 to access and transmit location data from the mobile device to Apple's servers, and indeed, such data about Plainitffs Gupta and Rodimer was being continuously transmitted without users' knowledge or consent.

143. Even more shocking, the information collected and sent from users' iPhones to

[12] *See*, Apple Letter to Representatives Markey and Barton, http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf (last visited October 18, 2011).

Apple can easily be input into a publicly searchable database, which in turn reveals a very precise estimate of each users' exact location.

144. As a result, Apple—or anyone with access to this geolocational data—is able to approximate the exact location of thousands, if not millions, of United States citizens, including Plainitffs Gupta and Rodimer, even after these users unequivocally denied Apple with access to their geolocation information.

145. In April of 2011—after Plaintiff Gupta's initial lawsuit exposed Apple's unlawful tracking program—Apple finally admitted that its iPhones were collecting and transmitting its users' geolocation information to its servers, even when users affirmatively opted out by turning their Location Service settings "Off". Rather than owning up to its misconduct and taking responsibility for it as it advertised, Apple chalked up its misconduct to "a bug, which [it] plan[s] to fix shortly."[13]

146. This admission plainly contradicts Apple's representations to its customers and Congress regarding the ability to opt-out of its geolocation tracking program.

147. Apple's attempt to blame its unauthorized tracking scheme on a software "bug" is far-fetched. Apple is one of the largest and most renowned software developers in the world, with a large and highly sophisticated staff of engineers. As explained below, the idea that Apple's software engineers mistakenly designed the iPhone software to ignore users' withdrawal of consent is untenable.

148. When developing iOS 4, Apple specifically included a mechanism (in programming parlance, a "method" named locationServicesEnabled that returns a boolean value) to determine whether or not users have disabled location services.[14] Apple requires third party

[13] Apple Q&A on Location Data, http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html (last visited October 18, 2011).

[14] Apple's iOS Developer Library, http://developer.apple.com/library/ios/#documentation/CoreLocation/Reference/CLLocationManager_Class/CLLocationManager/CLLocationManager.html#//apple_ref/occ/clm/CLLocationManager/locationServicesEnabled (last visited October 24, 2011).

App developers to utilize this mechanism before collecting location data from an iPhone to ensure consent has been properly obtained. Moreover, if a third party App provider disregards the customers' choice to disable location services and attempts to gather such data anyway, Apple designed iOS 4 to automatically prevent access to the data, and display a prompt to the customer informing the individual that an application is attempting to access location information.

149. These measures belie Apple's statements that it accidently collected location data without consent. Indeed, it appears that Apple took steps to circumvent *its own* failsafe procedures in order to collect and transmit location data without user consent.

150. In light of the programmatic design of iOS 4 described above, it becomes clear that Apple's unlawful behavior was not caused by a "bug" or coding error. To the contrary, Apple intentionally programmed its software to send its users' geolocation information to its servers, without consent, because it wanted to maximize the amount of data available for its digital marketing grid.

151. Apple further jeopardizes consumers' privacy interests by causing the geolocation data it collects to be automatically downloaded and stored on any device used to sync or back-up Plaintiffs and consumers' iPhone data, without ever informing Plaintiffs and consumers of that practice, obtaining their consent, or providing a mechanism to opt-out.

152. In addition, Apple caused the geolocation files it creates to be stored in a readily accessible, unencrypted form. As a result, Plaintiffs' geolocation data is accessible to any other person who may have access to a computer used to back-up one's iPhone.

153. Plaintiffs Gupta and Rodimer and the Geolocation Class have a legally protected interest in the privacy of their location and movements, for prolonged tracking of their movement can reveal an intensely intimate portrait of their lives.

154. That interest is objectively reasonable where, as here, Plaintiffs and consumers expressly opted out of Apple's geolocation tracking, by setting their Location Services setting to "Off."'

155. The electronic tracking of Plaintiffs and consumers' location and movements by Apple, without their knowledge—particularly after they expressly opted out of such tracking—

violates their reasonable expectation of privacy, particularly in light of Apple's representations that it would not permit access to, or the collection/transmission of such data.

156. The serious nature, scope and potential impact of such privacy invasions is tethered to a legislatively declared policy as expressed in California Penal Code Sec. 637.7, which makes it unlawful for anyone other than law enforcement to use an electronic tracking device to determine the location or movements of a person.

157. The potential impact of this privacy violation is further exacerbated by the fact that, unbeknownst to Plaintiffs Gupta and Rodimer and the Geolocation Class, Apple exposes the tracking data to anyone with access to any device that was used to back up iPhone data, which potentially subjects Plainitffs Gupta and Rodimer, and the Geolocation Class, to a host of harms, including stalking.

158. As a result of Apple's intentional privacy invasions, Plaintiffs Gupta and Rodimer and the Geolocation Class are entitled to statutory damages and/or other equitable relief under the Stored Communications Act (18 U.S.C. § 2701, *et seq*.), the Electronic Communications Privacy Act (18 U.S.C. § 2510, *et seq*.), and Art. I, section 1 of the California Constitution.

**F. The Tracking Defendants Exploit Access to Consumer Data**

159. Notwithstanding Apple's control of the user experience, it designs its mobile devices to be very open when it comes to disclosing information about consumers to the Tracking Defendants, companies that incentivize App developers to provide the App Store with free Apps for iDevices and provide Apple the metrics to support its claims of market leadership.

160. The personal and private information is of extreme interest to many advertising networks and web analytics companies, including the Tracking Defendants. For this reason, the Tracking Defendants pay to support App development, so that many Apps are provided to consumers ostensibly "free" or at a lower cost.

161. When users download and install the Apps on their iDevices, the Tracking Defendants' software accesses personal information on those devices without users' awareness or permission and transmits the information to the Tracking Defendants, supplying them with de-

tails such as consumers' cellphone numbers, address books, UDIDs, and geolocation histories—highly personal details about who the consumers are, who they know, what they do, and where they are.

162. Some Tracking Defendants pay App developers to include code that causes ads to be displayed when users run the apps. Those ads are then populated with content from the Tracking Defendants and provide the communications channel for the Tracking Defendants to acquire and upload users' personal information.

163. In the wake of Apple's prohibition against sending user information to third parties, described above, protests erupted from a number of third-party advertising networks and metrics/analytics companies (who have been receiving a steady flow of user data from iDevice Apps). One prominent critic was the CEO of Google-owned AdMob. Following this criticism, Apple has taken no steps to actually implement its changed Developer Agreement or enforce it in any meaningful way.

164. As a result, the Tracking Defendants, through the Apps with whom they had entered into relationships and to whom they had provided code, have continued to acquire details about consumers and to track consumers on an ongoing basis, across numerous applications, and tracking consumers when they accessed Apps from different mobile devices.

165. With the personal information acquired, the Tracking Defendants used the information to compile—in addition to the types of information described in paragraphs 58 through 68, above—personal, private, and sensitive information that included consumers' video application viewing choices, web browsing activities, and their personal characteristics such as gender, age, race, family status, education level, geographic location, and household income, even though the Tracking Defendants require none of this information to provide the user services for which the Apps were marketed.

166. The Tracking Defendants acquired personal information and compiled profiles that were unnecessary to the Apps' stated functions but were useful to the Tracking Defendants in their commercial compilation, use, and sale of consumers' personal information.

167. Because of Apple's and the Tracking Defendants' control and coding, Plaintiffs

and consumers are unable to detect, manage, or avoid this collection and transmittal of information.

168. Apple is aware that Apps are providing a conduit for the Tracking Defendants to acquire consumers' personal information without consumers' knowledge or consent.

169. However, because consumers are unaware of the Tracking Defendants, they cannot complain to Apple about particular Apps and request that Apple remove the apps from the App Store.

170. Apple has continued to allow App developers to run their apps on its iOS platform and failed to void the licensing agreements with App developers, even after it received notice of Tracking Defendants' practices.

**G. No Consent**

171. Plaintiffs in this action consider the information from and about themselves on their iDevices to be personal and private information.

172. Consumers using iDevices that download Apps from the App Store would reasonably consider information from and about themselves stored on their iDevices to be personal and private information that they would not expect to be collected and used by third parties without the consumers' express consent.

173. Plaintiffs did not expect, receive notice of, or consent to the Tracking Defendants tracking their App use. Plaintiffs did not expect, receive notice of, or consent to the Tracking Defendants acquisition of Plaintiffs' personally identifiable information.

174. The Tracking Defendants activities were in conflict with Apple's representations about what information third parties were permitted to access.

175. The Tracking Defendants actions exceeded the scope of any authorization that could have been granted by Plaintiffs at the time of downloading and using Apps.

176. Plaintiffs consider information about their mobile communications to be in the nature of confidential information.

177. Plaintiffs consider information about any website they visit, or Apps they download, to be in the nature of confidential information that they do not expect to be shared with an

unaffiliated company.

178. The Tracking Defendants sell users' personal information to, or purchase and merge user's personal information with, other personal information about the same users that is available in the commercial, secondary information market, which the traffickers take substantial efforts to shield from the public eye.

179. The Tracking Defendants and other parties to the information market use the merger of personal information to effectively or actually de-anonymize consumers.

180. Plaintiffs did not consent to being personally identified to the Tracking Defendants or for their personally identifiable information to be shared with and used on behalf of the Tracking Defendants.

181. The Tracking Defendants actions were knowing, surreptitious, and without notice and so were conducted without authorization and exceeding authorization.

182. The Tracking Defendants misappropriated Plaintiffs' personal information.

183. Consumers routinely engage in online economic exchanges with the websites they visit by exchanging their personal information for the websites' content and services in a value-for-value exchange, which reduces the costs consumers would otherwise have to pay.

184. This value-for-value exchange also takes place when an App is supported by advertising revenue, such as revenue the Tracking Defendants pay App developers.

185. Because the Tracking Defendants engaged in undisclosed and/or inadequately disclosed data collection from Plaintiffs, they did not receive the full value of their exchanges.

186. In essence, the Tracking Defendants raised the price Plaintiffs paid to use the App but, instead of telling them, the Tracking Defendants simply reach around (or through) the App and into Plaintiffs' pockets, extracting an undisclosed premium in the form of Plaintiffs' information.

187. Because Tracking Defendants imposed an undisclosed cost on Plaintiffs, by taking more information than they were entitled to take, the Tracking Defendants' practices imposed economic costs on Plaintiffs.

188. The scarcity of consumer information increases its value. The Tracking

Defendants devalued Plaintiffs' information by taking and propagating it.

189. The undisclosed privacy and information transfer consequences of the Tracking Defendants' practices imposed costs on consumers in the form of the loss of the opportunity to have entered into value-for-value exchanges with other App providers whose business practices better conformed to Plaintiffs and Class Members' expectations. Thus, the Tracking Defendants' failure adequately to disclose the information practices, and using the lack of disclosure as a cover for taking consumers' information, the Tracking Defendants imposed opportunity costs on Plaintiffs.

190. Likewise, the Tracking Defendants' lack of disclosure coupled with their taking of information imposed costs on Plaintiffs who would otherwise have exercised their rights to utilize the economic value of their information by declining to exchange it with Tracking Defendants or any other App provider.

191. Plainitffs' information, which they use as an asset of economic value in the ways described above, has discernible value as an asset in the information marketplace, where consumers may market their own information.

192. The Tracking Defendants' conduct alleged in this complaint constituted an ongoing course of conduct that harmed Plaintiffs and consumers in general, and caused them to incur financial losses.

193. The Tracking Defendants deprived Plaintiffs of and/or diminished the economic value of their personal information.

194. The Tracking Defendants used Plaintiffs' personal information for their own economic benefit.

195. The Tracking Defendants perpetrated the acts and omissions set forth in this complaint through an organized campaign of deployment, which constituted the same act.

196. Plaintiffs and Class Members have been harmed by the Tracking Defendants' deceptive acquisition of their personal information in the loss of their rights to use, share, and maintain the confidentiality of their information, each according to his or her own discretion.

**H. Tracking Defendants' Harmful Use of Plaintiffs' Resources**

197. In addition to the harms alleged above, the Tracking Defendants' unauthorized, surreptitious collection of Plaintiffs' information, as alleged in paragraphs 58 through 68, above subjected Plaintiffs to harms because the Tracking Defendants actions consumed resources to which Plaintiffs had the right of controls and use.

198. For example, in the course of the use of the Weather Channel App by Plaintiffs Burwick, Chiu, Freeman, Kimbrell, and Lalo, Defendant Medialets caused a compressed .zip file of approximately two megabytes in size to be downloaded to each of Plaintiffs' iDevices and for purposes unrelated to those expected in the Weather Channel App. In doing so, Defendant Medialets unexpectedly utilized such Plaintiffs' bandwidth resources for which Plaintiffs paid charges to their carriers, and consuming storage space on their iDevices, which Plaintiffs had purchased without expectation of such unauthorized resource use by Apps from the App Store.

199. As to all Tracking Defendants, their actions in collecting information from Plaintiffs utilized power resources on Plaintiffs' iDevices, against without disclosure or authorization.

200. The rate at which battery charge was diminished on the iDevices as a result of the Tracking Defendants' actions was material to Plaintiffs, particularly given the power resource constraints on the iDevice: the Tracking Defendants' repeated actions during App executions utilized approximately two to three seconds of battery capacity with each action due to the power requirements of CPU processing, file input and output actions, and Internet connectivity.

201. Not only did Tracking Defendants' actions cause Plaintiffs' iDevice batteries to discharge more quickly, rendering the iDevices less useful given power constraints, but the Tracking Defendants repeated actions also resulted in lasting impairment because, by repeatedly utilizing power and causing Plaintiffs to have to re-charge their iDevices batteries sooner, the Tracking Defendants shortened the actual utility and life of the iDevice batteries, for which charging capabilities are diminished over repeated re-chargings.

202. Quantification of the effect of the Tracking Defendants impairment of the utility of Plaintiffs' iDevice batteries and concomitant diminution in the value of the iDevices can be discerned through discovery of Apple and the Tracking Defendants and expert testimony.

## VI. CLASS ALLEGATIONS

203. Pursuant to the Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this action as a class action on behalf of themselves and all others similarly situated as members of the "iDevice Class," defined as follows:

> All persons residing in the United States who have purchased iPhones and downloaded free Apps from the App Store on a mobile device that runs Apple's iOS, from December 1, 2008 to the date of the filing of this Complaint.

204. In addition, Plaintiffs Gupta and Rodimer bring this action on behalf of themselves and of all others similarly situated as members of the "Geolocation Class," defined as follows:

> All individuals and entities in the United States and its territories that have turned off Location Services on their iPhones prior to April 27, 2011, and have unwittingly, and without notice or consent transmitted location data to Apple's servers, to the date of the filing of this Complaint.

205. Excluded from the iDevice Class and Geolocation Class are Defendants, their legal representatives, assigns, and successors, and any entities in which Defendants have controlling interests. Also excluded is the judge to who this case is assigned and the judge's immediate family.

206. The "Class Period" is December 1, 2008 to the present for the iDevice Class, and June 21, 2010 to April 27, 2011 for the Geolocation Class.

207. Plaintiffs reserve the right to revise the Class definitions based on facts learned in the course of litigating this matter.

208. The iDevice and Geolocation Classes each consist of millions of individuals and other entities, making joinder impractical.

209. The claims of Plaintiffs are typical of the claims of all other iDevice and Geolocation Class Members, respectively.

210. Plaintiffs will fairly and adequately represent the interests of the other iDevice Class Members, and Plaintiffs Gupta and Rodimer will fairly and adequately represent the interests of the other members of the Geolocation Class. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of iDevice and Geolocation Class, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interests adverse to those of the other iDevice or Geolocation Class Members.

211. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would have no effective remedy.

212. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

213. Defendants have acted and failed to act on grounds generally applicable to Plaintiffs and other Class Members, requiring the Court's imposition of uniform relief, including injunctive and declaratory relief, to ensure compatible standards of conduct toward the Class Members.

214. The factual and legal bases of Defendants' liability to Plaintiff and other Class Members are the same, resulting in injury to Plaintiff and all of the other Class Members. Plaintiffs and other Class Members have all suffered harm and damages as a result of Defendants' wrongful conduct.

215. There are many questions of law and fact common to Plaintiffs and the iDevice and Geolocation Class Members and those questions predominate over any questions that may affect individual Class Members. Common questions for the iDevice Class include, but are not limited to the following:

a. Whether Defendants, without authorization, tracked and compiled information to which iDevice Class Members enjoyed rights of possession superior to those of

Defendants;

b. Whether Defendants, without authorization, created personally identifiable profiles of iDevice Class Members;

c. Whether Defendants violated the statutes and common laws alleged herein;

d. Whether Defendants misappropriated valuable information assets of iDevice Class Members;

e. Whether Defendants caused economic harm to iDevice Class Members;

f. Whether Defendants created or caused or facilitated the creation of personally identifiable consumer profiles of iDevice Class Members;

g. Whether Defendants continue to retain and/or sell, valuable information assets from and about iDevice Class Members;

h. What uses of such information were exercised and continue to be exercised by Defendants;

i. Whether Apple breached fiduciary duties owed to Plaintiffs and iDevice Class Members;

j. Whether Defendants invaded and caused the invasion of the privacy of iDevice Class Members; and

k. Whether Defendants have been unjustly enriched.

216. There are many questions of law and fact common to Plaintiffs Gupta and Rodimer and the Geolocation Class Members, and those questions predominate over any questions that may affect individual Geolocation Class Members. Common questions for the Geolocation Class include, but are not limited to the following:

a. Whether Apple collected location data from iPhones even after the user turns "Off" the Location Services function;

b. Whether Apple profits, or intends to profit from. The collection of geolocation data described more fully herein;

c. Whether Apple has been unjustly enriched by Plainitffs Gupta and

Rodimer and the Geolocation Class; and

d. Whether Apple has breached its fiduciary duties to Plaintiffs Gupta and Rodimer and the Geolocation Class.

217. The questions of law and fact common to Geolocation Class Members predominate over any questions affecting only individual members, and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

## VII. CLAIMS FOR RELIEF

218. Based on the foregoing allegations, Plaintiffs' claims for relief include the following:

### FIRST CLAIM FOR RELIEF
### Violations of the Stored Communications Act (18 U.S.C. § 2701, *et seq*.)
### By Plaintiffs Gupta and Rodimer on Behalf of the Geolocation Class Against Apple

219. Plaintiffs Gupta and Rodimer incorporate Paragraphs 1-202, 204, and 206-217 as if fully set forth herein.

220. The Stored Communications Act (the "SCA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(12).

221. Pursuant to the SCA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their recipient.

222. Congress enacted the SCA to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99–541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

223. As such, the SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization. 18 U.S.C. § 2701(a).

224. Apple violated 18 U.S.C. § 2701(a)(1) by intentionally accessing its consumers' communications without authorization and obtaining and/or altering authorized access to a wire or electronic communication while in electronic storage by collecting temporarily stored location data from Plaintiff Gupta and the Geolocation Class's iPhones after Locations Services was turned "Off." In particular, Apple intentionally bypassed user consent and obtained access to a file (consolidated.db) located on the iPhone that temporarily stores location data. Apple had actual knowledge of, and benefited from, this practice.

225. Apple has violated 18 U.S.C. § 2701(a)(2) because it intentionally exceeded authorization to access consumers' communications and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage by collecting location data from Plaintiff s Gupta and Rodimer's and the Geolocation Class's iPhones after Locations Services was turned "Off." Apple had actual knowledge of, and benefited from, this practice.

226. As a result of Apple's conduct described herein, and its violation of § 2701, Plaintiffs Gupta and Rodimer and the Geolocation Class have suffered injuries. Plaintiffs Gupta and Rodimer, on their own behalf and on behalf of the Geolocation Class, seek an order enjoining Apple's conduct described herein and awarding themselves and the Geolocation Class the maximum statutory and punitive damages available under 18 U.S.C. § 2707.

**SECOND CLAIM FOR RELIEF**
**Violations of the Electronic Communications Privacy Act (18 U.S.C. § 2510, *et seq.*)**
**By Plaintiffs Gupta and Rodimer and the Geolocation Class Against Apple**

227. Plaintiffs Gupta and Rodimer incorporate Paragraphs 1-202, 204, 206-217, and 220-226 as if fully set forth herein.

228. The Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* (the "ECPA") defines "electronic communications system" as any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communica-

tions, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

229. The ECPA broadly defines the "contents" of a communication, when used with respect to any wire, oral, or electronic communications, to include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

230. Apple violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting and endeavoring to intercept Plaintiffs Gupta and Rodimer's and the Geolocation Class' wire and/or electronic communications to, from, and within their iPhones.

231. Apple also violated 18 U.S.C. § 2511(1)(d) by intentionally using, and endeavoring to use the contents of Plaintiffs Gupta and Rodimer's and the Geolocation Class' wire and/or electronic communications to profit from its unauthorized collection and sale of Plaintiffs location data, despite knowing and having reason to know, that the information was obtained through interception of an electronic communication.

232. Apple intentionally obtained and/or intercepted, by device or otherwise, these wire and/or electronic communications, without the knowledge, consent or authorization of Plaintiffs Gupta and Rodimer or the Geolocation Class.

233. Plaintiffs Gupta and Rodimer and the Geolocation Class suffered harm as a result of Apple's violations of the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Apple as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

**THIRD CLAIM FOR RELIEF**
**Violations of the California Constitution, Art. I, Section 1 (Right to Privacy)**
**By Plaintiffs Gupta and Rodimer on Behalf of the Geolocation Class Against Apple**

234. Plaintiffs Gupta and Rodimer incorporate Paragraphs 1-202, 204, 206-217, 220-226, and 228-233 by reference as if fully set forth herein

235. Apple tracked the location and movement of Plaintiffs Gupta and Rodimer and the Geolocation Class via their iPhones, over a substantial period of time, without their knowledge or consent, and in violation of their express wishes, once they opted out of Apple's Location Services function.

236. In addition, Apple exposed its geolocation tracking data about Plaintiffs Gupta and Rodimer and the Geolocation Class to any third party who may access any device used to synchronize or back-up Plaintiffs Gupta and Rodimer's and the Geoloction Subclass' iPhone data.

237. Worse yet, Apple caused the geolocation files to be stored in a readily accessible, unencrypted form, which does not comply with reasonable standards for the transmittal of sensitive data.

238. Apple's conduct in electronically tracking consumers, and exposing that data to other third parties, is not a standard, legitimate commercial practice. Rather it is an egregious breach of industry standards[15], social norms, and is prohibited by law.

239. Plaintiffs Gupta and Rodimer and the Geolocation Class have a legally protected interest in information about their location and movements.

240. Under the circumstances here, where they opted out of Apple's Location Services function, Plaintiff Gupta and the Geolocation Class have an objectively reasonable expectation of privacy from being electronically tracked by Apple.

241. Apple has and continues to commit serious invasions of Plaintiffs Gupta and Rodimer's and the Geolocation Class' privacy, by tracking their location and movements, and/or by making the geolocation data available to any third party who may have access to any

[15] *See* n.7, 8 at 16, above.

device used to sync or back up Plaintiffs Gupta and Rodimer's and the Geolocation Class' iPhones.

242. Accordingly, Plaintiff Gupta and the Geolocation Class seek declaratory and injunctive relief to prevent Apple from continuing to track and expose their location information.

**FOURTH CLAIM FOR RELIEF**
**Violations of the California Constitution, Art. I, Section 1 (Right to Privacy)**
**By Plaintiffs, and on behalf of the iDevice Class, Against All Defendants**

243. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, and 205-217 by reference as if fully set forth herein.

244. Plaintiffs have a legally protected privacy interest in their electronic communications and in the highly detailed and confidential personal information that was obtained, without their knowledge or consent, by Apple and the Tracking Defendants.

245. Under the circumstances here, where Apple made the above described misrepresentations about its control over and measures taken to protect the privacy and security of Plaintiffs' information interests with respect to the iDevice and the Apps, where Apple and the Tracking Defendants provided no notice of their clandestine tracking activities, where the iDevice is used in all facets of Plaintiffs and Class Members lives as described above, and in consideration of the highly detailed and confidential nature of, and in some instances, personally identifiable nature of the information taken by Defendants, Plaintiffs and Class Members had an objectively reasonable expectation of privacy from being electronically tracked by Apple and the Tracking Defendants, and from the disclosure of their personal information to the Tracking Defendants.

246. Apple's conduct, which by design, allowed the Tracking Defendants to obtain their personal information, is not a standard, legitimate commercial practice. Rather it is an egregious breach of industry standards, social norms, and is prohibited by law. Apple and the Tracking Defendants have and continue to commit these serious invasions of Plaintiffs and the Class' privacy.

247. There are no competing or countervailing interests that outweigh the privacy interests at stake. Accordingly, Plaintiffs and the iDevice Class seek declaratory and injunctive

relief to prevent Apple and the Tracking Defendants from continuing to track and expose their personal information and electronic communications

**FIFTH CLAIM FOR RELIEF**
**Negligence**
**By the Plaintiffs on Behalf of the Classes Against Apple**

248. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, and 244-247 by reference as if fully set forth herein.

249. As set forth above, Apple owed a duty to Plaintiffs and Class Members to protect their personal information and data property, and take reasonable steps to protect them from the wrongful taking of their personal information and the wrongful invasion of their privacy.

250. This duty is not based on any contractual obligation, but arises as a matter of law because Apple has at all times been aware of the likelihood of harm that would occur should it fail to act reasonably under the circumstances described above. Apple has an independent duty to avoid reasonable harm to others that it reasonably foresees might be harmed by those actions.

251. Apple also has a duty as the proprietor of its App Store, which is the functional equivalent any other traditional business establishment, to protect its patrons from, or at least warn of, harm from third parties that Apple reasonably foresees—particularly where the harm is not evident to Plaintiffs. Such a duty arises out of the special relationship between Apple and Plaintiffs.

252. Apple, having exercised total control over the App approval process, and indeed the entire Apple user experience, undertook a duty to protect Plaintiffs from the harmful actions that Apple knew would be caused by the use of Apps, and had an obligation to use reasonable care to prevent such harm or to adequately warn Plaintiffs of such harm.

253. Apple breached its duty by designing iDevices so that the Tracking Defendants could acquire personal information without Plaintiffs' knowledge or permission, by failing to review and remove privacy-violating apps from the App Store, and by constructing and controlling consumers' user experience and mobile environment so that consumers could not reasona-

bly avoid such privacy-affecting actions.

254. Apple failed to fulfill its own commitments and, further, failed to fulfill even the minimum duty of care to protect Plaintiff and Class Members' personal information, privacy rights, and security.

255. Apple's failure to fulfill its commitments included Apple's practice of capturing frequent and detailed information about iDevice users' locations for up to one year, including the locations of iDevice users who had utilized Apple's prescribed method for disabling Global Positioning System services, and

a. maintaining records of such location histories on users' iDevices,

b. transferring such location history files to users' replacement iDevices, and to other computers with which users synchronized their iDevices,

c. storing such location history files in accessible, unencrypted form,

d. without providing notice to users or obtaining users' consent,

e. where consumers had no reasonable means to become aware of such practice or to manage it, and

f. where such practice placed users at unreasonable risk of capture and misuse of such highly detailed and personal information.

256. Any reasonable consumer, including Plaintiffs would consider such a practice unexpected, objectionable, and shocking to the conscience of a reasonable person.

257. Plaintiffs and Class Members were harmed as a result of Apple's breaches of its duties, which damage is separate and apart form any damage to their iPhones themselves.

258. Apple proximately caused such harms, which were a reasonably foreseeable result of Apple's negligence.

**SIXTH CLAIM FOR RELIEF**
**Violations of the Computer Fraud and Abuse Act (18 U.S.C § 1030, *et seq.*)**
**By Plaintiffs Gupta and Rodimer on Behalf of the Geolocation Class Against Apple**

259. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, and 249-258 by reference as if fully set forth herein.

260. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA,"

regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

261. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA."

262. Apple violated 18 U.S.C. 1030 by intentionally accessing Plaintiffs' and Class Members' iDevices without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

263. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

264. Apple violated the CFAA in that it caused the transmission to users' iDevices, either by native installation or iOs upgrade, of code that caused users' iDevices to maintain, synchronize, and retain detailed, unencrypted location history files.

265. Apple knowingly and intentionally designed its iOS 4 software to retrieve and transmit geolocation information located on its customers' iPhones to Apple's servers and to do so even if the user has disabled the iDevice's Location Services GPS features.

266. Apple intended to cause damage to Plaintiff and Class Members' iDevices in that it knew or should have known that its tracking activities would consume Plaintiffs and Class Members' valuable computer assets and resources, as described more fully above in paragraph 118 through 122.

267. Apple acted without authorization and/or exceeding authorization in that it continued to track and store location information about Plaintiffs Gupta and Rodimer, even when their iDevices' Location Services was set to "off."

268. Each of Plaintiffs and Class Members' mobile devices is a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18

U.S.C. § 1030(e)(2)(B).

269. Apple violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a command to be downloaded to Plaintiffs' iDevices, which are protected computers as defined above, and intentionally causing damage without authorization.

270. Apple violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs' and Class Members' protected iDevices without authorization, and as a result of such conduct, recklessly causing damage to Plaintiffs and Class Members' iDevices by impairing the integrity of data and/or system and/or information.

271. Apple violated 18 U.S.C. § 1030 (a)(5)(A)(iii) by intentionally accessing Plaintiffs' and Class Members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiffs and Class Members.

272. As alleged above in paragraphs 118 through 122, Plaintiffs and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

273. As alleged above in paragraphs 118 through 122, Plaintiffs and Class Members have also suffered loss by reason of these violations, as defined in 18 U.S.C. 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

274. Apple's unlawful access to Plaintiff and Class Members' computers, use of their Computer Assets, interruption of their services, and taking of their location information was carried out through the same automated process, and resulted in an aggregated loss to Plaintiff and Class Members of at least $5,000 within a one-year period.

275. The aggregated losses to Plaintiff and Class Members amount to $5,000 or greater during a one-year period in that the hard drive space consumed by Apple for its undisclosed geolocation file is equal to approximately twenty-three cents ($0.23) per iDevice. The

Geolocation Class consists of millions of individuals. When losses are aggregated amongst Plaintiff and one million class members, losses equal $230,000.

276. Apple's unlawful access to Plaintiffs' and Class Members' computers and electronic communications has caused Plaintiffs and Class Members irreparable injury. Unless restrained and enjoined, Apple will continue to commit such acts. Plaintiff's and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

**SEVENTH CLAIM FOR RELIEF**
**Violations of the Computer Fraud and Abuse Act (18 U.S.C § 1030, *et seq.*)**
**By Plaintiffs on Behalf of the iDevice Class Against All Defendants**

277. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, 249-258, and 260-276 by reference as if fully set forth herein.

278. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

279. Defendants violated 18 U.S.C. 1030 by intentionally accessing Plaintiffs' and Class Members' iDevices without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

280. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA."

281. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

282. Defendants violated the CFAA in that they caused the transmission of code or commands to Plaintiffs and Class Members' iDevices, which code or commands accessed the

personal information of Plaintiffs and Class Members and transmitted such information to Tracking Defendants.

283. Each of Plaintiffs and Class Members' mobile devices is a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

284. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a command to be downloaded to Plaintiffs' iDevices, which are protected computers as defined above, and intentionally causing damage without authorization.

285. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs' and Class Members' protected iDevices without authorization, and as a result of such conduct, recklessly causing damage to Plaintiffs and Class Members' iDevices by impairing the integrity of data and/or system and/or information.

286. Defendants violated 18 U.S.C. § 1030 (a)(5)(A)(iii) by intentionally accessing Plaintiffs' and Class Members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiffs and Class Members.

287. Defendants intended to cause damage in that they knew or should have known that their conduct would consume Plaintiffs and Class Members' valuable computer assets and resources, as described more fully above in paragraphs 197 through 202.

288. Defendants intended to access Plaintiff and Class Members' computers and personal information, inasmuch as such access was accomplished through the execution of computer code and instructions specifically designed for such access, such as App code created using Tracking Defendants' and Apple's SDKs, which effected access of Plaintiffs' and Class Members' computers by interacting with Apple-provided APIs (application programming interfaces) specifically designed by Apple to facilitate the retrieval of information from iDevices.

289. Defendants' conduct was without authorization and/or exceeding authorization.

290. Plaintiffs and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

291. As alleged above in paragraphs 178 through 193, and 196, Plaintiffs and Class Members have suffered loss by reason of these violations, as defined in 18 U.S.C. 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

292. Defendants' unlawful access to Plaintiff and Class Members' computers, use of their computer assets and resources, interruption of their services, and taking of their information was carried out through the same automated process, and resulted in an aggregated loss to Plaintiff and Class Members of at least $5,000 within a one-year period.

293. The aggregated losses to Plaintiff and Class Members amounts to $5,000 or greater during a one-year period in that the battery life consumed by Tracking Defendants, and the concomitant diminution in the value of the iDevices, can be discerned through discovery of Apple and the Tracking Defendants and expert testimony. The iDevice Class consists of millions of individuals whose losses are a function of repeated, battery-affecting App events. When losses are aggregated across Plaintiffs and one million class members, losses exceed $5,000 during any one-year period during the Class Period.

294. Defendants' unlawful access to Plaintiffs' and Class Members' computers and electronic communications has caused Plaintiffs and Class Members irreparable injury. Unless restrained and enjoined, Tracking Defendants will continue to commit such acts. Plaintiffs' and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

295. Each Defendant is jointly and severally liable for the conduct alleged hereunder of any other Defendants and/or Defendants.

**EIGHTH CLAIM FOR RELIEF**
**Trespass**
**By Plaintiffs on Behalf of the Classes Against All Defendants**

296. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, 249-258, 260-276, and 278-295 by reference as if fully set forth herein.

297. The common law prohibits the intentional intermeddling with personal property, including an iDevice, in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

298. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiffs and Class Members, Defendants dispossessed Plaintiffs and Class Members from use and/or access to their iDevices, or parts of them, by surreptitiously adding harmful iDevice functions and the execution of harmful privacy-affecting code.

299. Further, these acts materially impaired the use, value, and quality of Plaintiffs and Class Members' iDevices. Defendants' acts constituted an intentional interference with the use and enjoyment of the iDevices. By the acts described above, Defendants repeatedly and persistently engaged in trespass to personal property in violation of the common law.

300. Without Plaintiffs and Class Members' consent, or in excess of any consent given, Defendants knowingly and intentionally accessed and/or caused the access to Plaintiffs' and Class Members' property, thereby intermeddling with Plaintiffs' and Class Members' right to possession of the property and causing injury to Plaintiffs and the members of the Class.

301. Defendants engaged in deception and concealment to gain access to Plaintiffs and Class Members' iDevices.

302. Defendants engaged in the following conduct with respect to Plaintiffs and Class Members' iDevices: Defendants accessed and obtained control over iDevices; Defendants caused the installation of code on the hard drives of the iDevices; Defendants programmed the operation of its code to circumvent the iDevice owners' privacy and security controls to remain beyond their control, and to continue function and operate without notice to them or consent from Plaintiff and Class Members.

303. All these acts described above were acts in excess of any authority any user granted at any time and none of these acts was in furtherance of users' uses of iDevices or Apps. By engaging in deception and misrepresentation, whatever authority or permission Plaintiffs and Class Members may have granted to the Defendants did not apply to Defendants' conduct.

304. Defendants' installation and operation of its program used, interfered, and/or intermeddled with Plaintiffs' and Class Members' iDevice systems. Such use, interference and/or intermeddling was without Class Members' consent or, in the alternative, in excess of Plaintiffs' and Class Members' consent.

305. Defendants' installation and operation of its program constitutes trespass, nuisance, and an interference with Class Members' chattels, to wit, their iDevices.

306. Defendants' installation and operation of its program materially impaired the condition and value of Class Members' iDevices.

307. Defendants' trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and Class Members.

308. As a direct and proximate result of Defendants' trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiffs and Class Members' property, Defendants has injured and impaired in the condition and value of Class Members' iDevices, as follows:

a. by consuming the resources of and/or degrading the performance of Plaintiffs' and Class Members' iDevices (including hard drive space, memory, processing cycles, and Internet connectivity);

b. by diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiffs' and Class Members' iDevices;

c. by devaluing, interfering with, and/or diminishing Plaintiffs' and Class Members' possessory interest in their iDevices;

d. by altering and controlling the functioning of Plaintiffs' and Class Members' iDevices;

e. by infringing on Plaintiffs' and Class Members' right to exclude others from their iDevices;

f. by infringing on Plaintiffs' and Class Members' right to determine, as owners of their iDevices, which program functionality should be installed and operating on their iDevices;

g. by compromising the integrity, security, and ownership of Class Members' iDevices; and

h. by forcing Plaintiffs' and Class Members' to expend money, time, and resources in order to remove the program installed on their iDevices without notice or consent.

309. Each Defendant is jointly and severally liable for the conduct alleged hereunder of any other Defendants and/or Defendants.

**NINTH CLAIM FOR RELIEF**
**Violations of the Consumers Legal Remedies Act (California Civil Code § 1750, *et seq.*)**
**By Plaintiffs on Behalf of the Classes Against Apple**

310. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, 249-258, 260-276, 278-295, and 297-309 by reference as if fully set forth herein.

311. The California Consumer Legal Remedies Act, Section 1750 of the California Civil Code (the "CLRA") protects consumers against fraud, unlawful practices, and unconscionable commercial practices in connection with sale of any merchandise.

312. In violation of the CLRA, Defendant Apple has engaged and is engaging in unfair and deceptive acts and practices in the course of transactions with Plaintiffs, and such transactions are intended to and have resulted in the sales of goods to consumers.

313. Plaintiffs and the Class Members are "consumers" as that term is used in the CLRA because they sought or acquired Defendant's goods, *i.e.*, Apple's iDevices, for personal, family, or household purposes. Defendant's past and ongoing acts and practices include but are not limited to Defendant's representation that its goods were of a particular standard, quality, and grade when in fact, they were of another.

314. In particular, as described in paragraphs 139 and 140 above, Apple represented to Plaintiffs Gupta and Rodimer and members of the Geolocation Class that they could prevent

Apple from collecting geolocation data about them by switching the Location Services setting on their iPhones to "Off," when, in fact, Apple continued to track and store locations information about them even when Location Services was set to "off."

315. Apple also made the following representations, expressly or by implication, to Plaintiffs and members of the iDevice Class about the iDevice and the Apple ecosystem: (a) Apple designed the iPhone to safely and reliably download third party Apps; (b) certain Apps available for download by users in the App store are "free Apps;" (c) the App Store does not permit Apps that "violate[] our developer guidelines" including Apps containing pornography, Apps that violate a users privacy, and Apps that hog bandwidth; (c) "Apple takes precautions — including administrative, technical, and physical measures — to safeguard [users'] personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction;" (d) Apple does not allow one App to access data stored by another App; and (e) Apple does not allow an App to transmit data from a user's iDevice to other parties without the user's consent.

316. These representations were materially misleading and failed to disclose the following material facts: (a) the Apps downloaded by Plaintiffs and the iDevice Class are not "free" in so far as Apple and the Tracking Defendants obtain Plaintiffs and Class Members' valuable information assets, and consume their bandwidth and iDevice resources, without consent or notice, as described above; (b) Apple knowingly permits Apps that subject Plaintiffs and Class Members to privacy exploits and security vulnerabilities to be offered in the App Store; and (c) Apple does not analyze the traffic generated by Apps to detect Apps that violate the privacy terms of the iOS Developer Agreement and Apple's commitments to users.

317. Plaintiffs and Class Members would not have purchased their iDevices and/or would not have paid as much for them, if Apple had disclosed the true facts that it and the Tracking Defendants would surreptitiously obtain personal information from their iDevices, track their activity and geolocation, and consume portions of the "cache" and/or gigabytes of memory on their devices—memory that Plaintiffs paid for the exclusive use of when they purchased their iDevice.

318. Because Apple did not disclose the true costs of their iDevices, Plaintiffs were misled into purchasing a product that did not meet their reasonable expectations.

319. Given the undisclosed costs imposed by using the iDevice, it was not useful to Plaintiffs and was not as valuable to them as the price for which they paid for it.

320. Plaintiffs and members of the Classes relied upon and were deceived by Apple's with material misrepresentations and omissions regarding the iDevice.

321. As a proximate and direct result of Apple's misrepresentations, omissions, and unlawful and unconscionable commercial practices, Plaintiffs and members of the Class have been injured and suffered damages in that they have purchased products that invade their privacy, render their personal information insecure, consume their valuable device storage and power resources as well as their Internet bandwidth, and are therefore less valuable products than that which they paid.

322. Defendant's violations of Civil Code § 1770 have caused damage to Plaintiffs and the other Class Members and threaten additional injury if the violations continue. This damage includes the privacy and economic consequences set forth above, including the purchase price or premium paid for the iDevice.

323. Pursuant to California Civil Code §1782, one or more of the Plaintiffs notified Defendant Apple in writing of the particular violations of Civil Code §1770 and demanded that it rectify the problems associated with their behavior detailed above, which acts and practices are in violation of Civil Code §1770. Apple failed to respond to that letter.

Plaintiffs request actual damages, restitution of property, punitive damages, injunctive relief and other relief that the Court deems proper, and reasonable attorneys' fees and costs, as permitted by Civil Code, Sections 1780 and 1782.

**TENTH CLAIM FOR RELIEF**
**Violations of the Unfair Competition Law (Cal. Bus. and Prof. Code § 17200, *et seq.*)**
**By Plaintiffs on Behalf of the Classes Against Apple**

324. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, 249-258, 260-276, 278-295, 297-309, and 311-323 by reference as if fully set forth herein.

325. Apple's acts and practices as detailed herein constitute acts of unfair competition. Apple has engaged in unlawful, unfair or fraudulent business acts and/or practices within the meaning of California Business & Professions Code, section 17200, et seq. Apple need only violate one of the three prongs to be held strictly liable.

**A. Unlawful Business Act and Practices**

326. Apple's business acts and practices are unlawful, in part, because they violate California Business and Professions Code, Section 17500, *et seq.*, which prohibits false advertising, in that they were untrue and misleading statements relating to Apple's provision of goods and with the intent to induce consumers to enter into obligations relating to such goods, and regarding which statements Apple knew or which, and by the exercise of reasonable care Apple knew or should have known, were untrue and misleading.

327. Apple's business acts and practices are also unlawful in that, as set forth herein, they violate the Consumer Legal Remedies Act, California Civil Code, Section 1750, *et seq.*; the False Advertising, California Business and Professions Code, Section 17500; the Computer Fraud and Abuse Act, Title 18, United States Code, Section 1030, *et. seq.*, the Stored Communications Act, 18 U.S.C. § 2701; and the Electronic Communications Privacy Act, 18 U.S.C. § 2510.

328. Apple's business acts and practices are also unlawful in that they violate the California Constitution, Article I, Section 1, which articulates the inalienable right to pursue and obtain privacy, in that Apple interfered with and obstructed users' rights and reasonable expectations regarding their privacy, particularly in light of promises made by Apple as an inducement for Plaintiffs and Class Members to purchase iDevices and download Apps.

329. Plaintiffs reserve the right to identify additional provisions of the law violated by Apple as further investigation and discovery warrants.

330. Apple is therefore in violation of the unlawful prong of the Unfair Competition Law.

**B. Unfair Business Act and Practices**

331. Apple's business acts and practices are unfair because they have caused harm and injury-in-fact to Plaintiff and Class Members and for which Apple has no justification other than to increase, beyond what Apple would have otherwise realized, its market share and revenue from sales of iDevices.

332. Apple's conduct lacks reasonable and legitimate justification in that it has benefited from such conduct and practices while Plaintiff and the Class Members have been misled as to the nature and integrity of Apple's iDevices and have, in fact, suffered material disadvantage regarding their interests in the privacy, confidentiality, and security of their personal information, in which they have a property interest, and have lost money, including the purchase price of the iDevice or, at a minimum, the difference of the inflated price and the price Apple should have charged for a product that fully disclosed all the costs hidden by Apple.

333. Apple's conduct offends public policy in California tethered to the Consumer Legal Remedies Act, the state constitutional right of privacy, and California statutes' recognition of the need for consumers to be information and equipped to protect their own privacy interests, such as California Civil Code, Section 1798.8, such that consumers may make informed decisions in their choices of merchants and other means of safeguarding their privacy.

334. In addition, Apple's *modus operandi* constitutes a sharp practice in that it knew or should have known that consumers care about the status and security of personal information and privacy but are unlikely to be aware of and able to detect the means by which Apple was conducting itself in a manner adverse to its commitments and users' interests, through the undisclosed functions of iDevices and Apps and the related conduct of the Tracking Defendants. Apple is therefore in violation of the unfairness prong of the Unfair Competition Law.

**C. Fraudulent Acts and Practices**

335. Apple's acts and practices were fraudulent within the meaning of the Unfair Competition Law because they were likely to mislead the members of the public to whom they were directed.

336. Apple's practice of (a) capturing, storing, and transferring through synchroniza-

tion to other computers highly detailed and personal records of users' location histories of long duration, and storing such information in unencrypted form; and (b) subjecting Plaintiffs to Apps that were linked to data collection by Tracking Defendants, which collection was accomplished by commandeering Plaintiffs' paid-for resources, was in violation of the unfairness prong of the Unfair Competition Law.

337. By engaging in the above-described acts and practices, Apple has committed one or more acts of unfair competition within the meaning of the Unfair Competition Law and, as a result, Plaintiffs and the Class have suffered injury-in-fact and have lost money and property—specifically, personal information; the private and secure use of the iDevices and Apps; and the expected utility and performance of their iDevices; and purchase price of the iDevice or, at a minimum, the difference of the inflated price and the price Apple should have charged for a product that fully disclosed all the costs hidden by Apple.

338. Apple had a duty to disclose the material privacy and security characteristics of the iDevice and its operation with the Apple-controlled ecosystem, including with Apps from the App Store, because it (i) knew or should have known about such characteristics at the time that Plaintiffs and members of the Class purchased the product, inasmuch as Apple created the iDevice, the App Store, and reviewed App Store offerings; (ii) had exclusive knowledge of these material facts, which information was not known to Plaintiffs; and (iii) made a partial representation as to the iDevice's integrity in promoting Plaintiffs' privacy and security interests and interests in the reasonably expected utility of their iDevices, but failed to disclose the material fact that the iDevice, the App Store, the Apps, and the entire Apple ecosystem and system of relationships with developers and Tracking Defendants was designed to foster the unauthorized taking of and profiting from Plaintiffs' personal information.

339. Plaintiffs and members of the Class were deceived by Apple's representations; and they reasonably relied on Apple's representations as described above, and the absence of any warning about about the characteristics and conditions that injured them, as alleged herein.

340. Plaintiffs and members of the Class have suffered injuries as a direct and proximate result of the unlawful, unfair, and fraudulent business practices of Apple.

341. Pursuant to section 17203 of the California Business and Professions Code, Plaintiffs, on their own behalf and on behalf of the Classes, Plaintiffs seek restitution and a Court order enjoining Defendants from such future conduct and any other such orders that maybe necessary to rectify the unlawful, unfair, and fraudulent business practices of Apple.

**ELEVENTH CLAIM FOR RELIEF**
**Violations of the Stored Communications Act (18 U.S.C. § 2701, *et seq*.)**
**By Plaintiffs on Behalf of the iDevice Class Against All Defendants**

342. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, 249-258, 260-276, 278-295, 297-309, 311-323, and 325-341 by reference as if fully set forth herein.

343. The Stored Communications Act (the "SCA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(12).

344. Pursuant to the SCA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their recipient.

345. Congress enacted the SCA to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99–541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

346. As such, the SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization. 18 U.S.C. § 2701(a).

347. Defendants violated 18 U.S.C. § 2701(a)(1) by intentionally accessing its consumers' communications without authorization and obtaining and/or altering authorized access to a wire or electronic communication while in electronic storage by collecting temporarily

stored location data from the iDevice Class' iPhones as set forth in paragraphs 58 through 64, above.

**TWELFTH CLAIM FOR RELIEF**
**Conversion**
**By Plaintiffs on Behalf of the iDevice Class Against All All Defendants**

348. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, 249-258, 260-276, 278-295, 297-309, 311-323, 325-341, and 342-347 by reference as if set forth herein at length.

349. Defendants have taken Plaintiffs' and Class members' specific personal property in the form of unique data about them that is private and personal.

350. Plaintiffs and Class Members have been harmed by this exercise of dominion and control over their information, for which they have not been compensated, and by which Defendants have been unjustly enriched.

351. As a result of such actions of conversion, Plaintiffs seek recovery for damages and appropriate injunctive relief.

**THIRTEENTH CLAIM FOR RELIEF**
**Common Counts, Assumpsit, and Restitution**
**By Plaintiffs on Behalf of the iDevice Class Against All Defendants**

352. Plaintiffs incorporate Paragraphs 1-29, 33-137, 159-203, 205-217, 244-247, 249-258, 260-276, 278-295, 297-309, 311-323, 325-341, 342-347, and 349-351 by reference as if set forth herein at length.

353. Defendants entered into a series of implied at law contracts with Plaintiffs and the iDevice Class Members that resulted in money being had and received by Defendants at the expense of Plaintiffs under agreements in assumpsit.

354. Defendants engaged in conscious and deliberate conduct, as set forth above, that disappoints or frustrates Plaintiffs' and Class members' reasonable privacy expectations that are implied in such agreements.

355. Defendants have been unjustly enriched by the resulting profits enjoyed by Defendants as a result of such agreements. Plaintiffs' detriment and Defendants' enrichment were related to and flowed from the conduct challenged in this Complaint.

356. Under common law principles recognized in claims of common counts, unjust enrichment, restitution and/or assumpsit, Defendants should not be permitted to retain the benefits conferred upon them based on the taking of such data from Plaintiffs and Class Members and converting it into revenues and profits without providing compensation therefore.

357. Under the principles of equity and good conscience, Defendants should not be permitted to retain the benefits they have acquired through the unlawful conduct described above, and as between the two, Plaintiffs and the iDevice Class Members have a superior right to some or all of such monies attributable to the value of such data over Defendants.

358. Plaintiffs and members of the Class seek damages and restitutionary disgorgement of all profits or monies generated from such illegal acts, and the establishment of a constructive trust from which Plaintiffs and Class Members may seek restitution as to all such funds, revenues and benefits that Defendants have unjustly received as a result of their actions that rightfully belong to Plaintiffs and the Class.

359. Plaintiffs also seek declaratory relief as to the rights and responsibilities of all parties to such implied-at-law agreements.

## VIII. DEMAND FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment against Defendants and that the Court may:

A. certify this case as a Class action on behalf of the Classes defined above, appoint Plaintiffs as Class representatives, and appoint their counsel as Class counsel;

B. declare that Defendants' actions violate the statutes and common-law jurisprudence set forth above;

C. award injunctive and equitable relief as applicable to the Class *mutatis mutandis*, including:

i. prohibiting Defendants from engaging in the acts alleged above;

ii. requiring Defendants to provide reasonable notice and choice to consumers regarding Defendants' tracking, data collection, profiling, merger, and deanonymization activities;

iii. requiring Defendants to disgorge to Plaintiffs and Class Members or to whomever the Court deems appropriate all of Defendants' ill-gotten gains;

iv. requiring Defendants to delete all data from and about Plaintiffs and Class Members that it collected and/or acquired from third parties through the acts alleged above;

v. requiring Defendants to provide Plaintiffs and other Class Members reasonable means to decline, permanently, participation in Defendants' collection of data from and about them;

vi. enjoining Apple from acquiring, retaining, and transferring, whether in encrypted or unencrypted form, users' detailed location history;

vii. requiring Apple to seek express consent from Plaintiffs and other Class Members to capture, retain, and transfer location history information and, otherwise, to purge such information from all resident systems and identify parties that have accessed such information on users' iDevices and synchronized devices;

viii. awarding Plaintiffs and Class Members full restitution of all benefits wrongfully acquired by Defendants through the wrongful conduct alleged above; and

ix. ordering an accounting and constructive trust to be imposed on the data from and about Plaintiffs and Class Members and on funds or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendants;

D. award damages, including statutory damages where applicable, to Plaintiffs and Class Members in an amount to be determined at trial;

E. award restitution against Defendants for all money to which Plaintiffs and the

Class are entitled in equity;

F. restrain, by preliminary and permanent injunction, Defendants, its officers, agents, servants, employees, and attorneys, and those participating with them in active concert, from identifying Plaintiffs and Class Members' electronic communications, whether by personal or pseudonymous identifiers, and from monitoring, accessing, collecting, transmitting, and merging with data from other sources any information from or about Plaintiff and Class Members;

G. award Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees; pre- and post-judgment interest to the extent allowable; restitution; disgorgement and other equitable relief as the Court deems proper; compensatory damages sustained by Plaintiffs and the Class; statutory damages, including punitive damages; and permanent injunctive relief prohibiting Defendants from engaging in the conduct and practices complained of herein; and

H. for such other and further relief as this Court deems just and proper.

Date: November 21, 2011

Respectfully submitted,
KAMBERLAW, LLC

By: s/Scott A. Kamber
Scott A. Kamber (*pro hac vice*)
KAMBERLAW, LLC
Interim Class Counsel

SCOTT A. KAMBER (*pro hac vice*)
DAVID A. STAMPLEY (*pro hac vice*)
*skamber@kamberlaw.com*
*dstampley@kamberlaw.com*
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

DEBORAH KRAVITZ (SBN 275661)
dkravitz@kamberlaw.com
KAMBERLAW, LLP
141 North St.
Healdsburg, California 95448
Telephone: (707) 820-4247
Facsimile: (212) 202-6364

*Interim Class Counsel*

WILLIAM AUDET
JONAS P. MANN
MICHAEL A. MCSHANE
AUDET & PARTNERS LLP
221 Main Street, Suite 1460
San Francisco, California 94105
Telephone: (415) 568-2555
Facsimile: (415) 568-2556

*Plaintiffs' Liaison Counsel*

JAY EDELSON
jedelson@edelson.com
SEAN REIS
sreis@edelson.com
EDELSON MCGUIRE, LLC
350 N LaSalle St.
Chicago IL 60654,
Telephone: (312) 589-6370

RICHARD A. LOCKRIDGE
ROBERT K. SHELQUIST
rlockridge@locklaw.com
rshelquist@locklaw.com
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

JEFF S. WESTERMAN
jwesterman@milberg.com
MILBERG LLP
One California Plaza
300 South Grand Avenue, Ste 3900
Los Angeles, California 90071
Telephone: (213) 617-1200
Facsimilie: (213) 617-1975

PETER E. SEIDMAN
ANDREI V. RADO
ANNE MARIE VU (Bar No. 238771)
pseidman@milberg.com
arado@milberg.com
avu@milberg.com
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

JEREMY WILSON
jeremy@wtlfirm.com
WILSON TROSCLAIR & LOVINS
302 N. Market Street, Suite 501
Dallas, Texas 75202
Telephone: (214) 430-1930

*Plaintiffs' Executive Committee*

JOSEPH MALLEY
malleylaw@gmail.com
LAW OFFICE OF JOSEPH MALLEY
1045 North Zang Blvd
Dallas TX 75208
Telephone: (214) 943-6100

DAVID PARISI
dcparisi@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Dr.
Sherman Oaks, CA 91403
Telephone: (818) 990-1299

MAJED NACHAWATI
mn@fnlawfirm.com
FEARS NACHAWATI LAW FIRM,
4925 Greenville Ave
Dallas TX 75206
Telephone: (214) 890-0711

JOHN F. NEVARES, ESQ.
CAMILO K. SALAS, III
jfnevares@nevareslaw.com
JOHN F. NEVARES & ASSOCIATES, P.S.C
P.O. Box 13667
San Juan
Puerto Rico

DANIEL E. BECNEL, JR.
dbecnel@becnellaw.com
NEVARES, BECNEL, SALAS
106 West Seventh Street
P.O. Drawer H
Reserve, Louisiana 70084
Telephone: (985) 536-1186

E. KIRK WOOD
ekirkwood1@bellsouth.net
WOOD LAW FIRM, LLC
P.O. Box 382434
Birmingham, AL 35238-2434;
Telephone: (205) 612-0243

JOSEPH WHATLEY
jwhatley@wdklaw.com
WHATLEY, DRAKE & KALLAS, LLC
2001 Park Place North, Suite 1000
Birmingham, Alabama 35203
Telephone: (205) 328-9576
Facsimile: (205) 328-9669

JERROLD PARKER
Jerry@yourlawyer.com
PARKER WAICHMAN & ALONSO, LLP
6 Harbor Park Drive
Port Washington, NY 11050
Telephone: (516) 466-6500

FRED ROSENTHAL
frosenthal@yourlawyer.com
PARKER WAICHMAN & ALONSO, LLP
111 Great Neck Road,
Great Neck, NY 11021
Telephone: (516) 466-6500

JOHN GOODSON
KEIL & GOODSON
611 Pecan
Texarkana, TX 75501
Telephone: (870) 772-4113

ALAN MANSFIELD
alan@clgca.com
THE CONSUMER LAW GROUP
9466 Black Mountain Road
San Diego CA 92126
Telephone: (619) 308-5034

THOMAS MAURIELLO
tomm@maurlaw.com
MAURIELLO LAW FIRM APC
1181 Puerta Del Sol
San Clemente, CA 92673
Telephone: (949) 542-3555

DONALD CHIDI AMAMGBO
donald@amamgbolaw.com
AMAMGBO & ASSOCIATES
6167 Bristol Parkway
Culver City, CA 90230
Telephone: (310) 337-1137

REGINALD VON TERRELL
reggiet2@aol.com
THE TERRELL LAW GROUP
PO Box 13315
MPB # 148
Oakland CA 94661
Telephone: (510) 237-9700

GILLIAN L WADE
gwade@milsteinadelman.com
SARA D AVILA
savila@milsteinadelman.com
CORINA N. MACCARIN
MILSTEIN ADELMAN & KREGER LLP
2800 Donald Douglas Loop N
Santa Monica, CA 90405
Telephone: (310) 396-9600

RICHARD PROAPS
rproaps@aol.com
RICHARD ALAN PROAPS, ATTORNEY AT LAW
8150 Greenback Lane,
Fair Oaks, CA 95628
Telephone: (916) 722-4881

AARON C. MAYER
aaron@mayerlawgroup.com
MAYER LAW GROUP
18 Carolina St.
Charleston, SC 29403
Telephone: (843) 376-4929

HOWARD RUBINSTEIN
LAW OFFICES OF HOWARD W. RUBINSTEIN
1615 Forum Pl.
West Palm Beach, FL 33401
Telephone: (832) 715-2788;

BRIAN SMITH
bws@smithvanture.com
SMITH & VANTURE, LLP
1615 Forum Pl.
West Palm Beach, FL 33401
Telephone: (561) 684-6330

MONICA KELLY
monicakelly@ribbecklaw.com
RIBBECK LAW CHARTERED
505 North Lake Shore Drive
Chicago, IL 60611
Telephone: (312) 822-9999

ERIC QUETGLAS-JORDAN
eric@quetglaslaw.com
QUETGLAS LAW OFFICE
PO Box 16606
San Juan, PR 00908-6606
Telephone: (787) 722-7745

*Counsel for Plaintiffs*

**JURY TRIAL DEMAND**

Plaintiff hereby demands a trial by jury of all issues so triable.

Date: November 21, 2011

Respectfully submitted,
KAMBERLAW, LLC

By: s/Scott A. Kamber
Scott A. Kamber (*pro hac vice*)
KAMBERLAW, LLC
Interim Class Counsel

SCOTT A. KAMBER (*pro hac vice*)
DAVID A. STAMPLEY (*pro hac vice*)
*skamber@kamberlaw.com*
*dstampley@kamberlaw.com*
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

DEBORAH KRAVITZ (SBN 275661)
dkravitz@kamberlaw.com
KAMBERLAW, LLP
141 North St.
Healdsburg, California 95448
Telephone: (707) 820-4247
Facsimile: (212) 202-6364

*Interim Class Counsel*

WILLIAM AUDET
JONAS P. MANN
MICHAEL A. MCSHANE
AUDET & PARTNERS LLP
221 Main Street, Suite 1460
San Francisco, California 94105
Telephone: (415) 568-2555
Facsimile: (415) 568-2556

*Plaintiffs' Liaison Counsel*

JAY EDELSON
jedelson@edelson.com
SEAN REIS
sreis@edelson.com
EDELSON MCGUIRE, LLC
350 N LaSalle St.
Chicago IL 60654,
Telephone: (312) 589-6370

RICHARD A. LOCKRIDGE
ROBERT K. SHELQUIST
rlockridge@locklaw.com
rshelquist@locklaw.com
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

JEFF S. WESTERMAN
jwesterman@milberg.com
MILBERG LLP
One California Plaza
300 South Grand Avenue, Ste 3900
Los Angeles, California 90071
Telephone: (213) 617-1200
Facsimilie: (213) 617-1975

PETER E. SEIDMAN
ANDREI V. RADO
ANNE MARIE VU (Bar No. 238771)
pseidman@milberg.com
arado@milberg.com
avu@milberg.com
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

JEREMY WILSON
jeremy@wtlfirm.com
WILSON TROSCLAIR & LOVINS
302 N. Market Street, Suite 501
Dallas, Texas 75202
Telephone: (214) 430-1930

*Plaintiffs' Executive Committee*

JOSEPH MALLEY
malleylaw@gmail.com
LAW OFFICE OF JOSEPH MALLEY
1045 North Zang Blvd
Dallas TX 75208
Telephone: (214) 943-6100

DAVID PARISI
dcparisi@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Dr.
Sherman Oaks, CA 91403
Telephone: (818) 990-1299

MAJED NACHAWATI
mn@fnlawfirm.com
FEARS NACHAWATI LAW FIRM,
4925 Greenville Ave
Dallas TX 75206
Telephone: (214) 890-0711

JOHN F. NEVARES, ESQ.
CAMILO K. SALAS, III
jfnevares@nevareslaw.com
JOHN F. NEVARES & ASSOCIATES, P.S.C
P.O. Box 13667
San Juan
Puerto Rico

DANIEL E. BECNEL, JR.
dbecnel@becnellaw.com
NEVARES, BECNEL, SALAS
106 West Seventh Street
P.O. Drawer H
Reserve, Louisiana 70084
Telephone: (985) 536-1186

E. KIRK WOOD
ekirkwood1@bellsouth.net
WOOD LAW FIRM, LLC
P.O. Box 382434
Birmingham, AL 35238-2434;
Telephone: (205) 612-0243

JOSEPH WHATLEY
jwhatley@wdklaw.com

WHATLEY, DRAKE & KALLAS, LLC
2001 Park Place North, Suite 1000
Birmingham, Alabama 35203
Telephone: (205) 328-9576
Facsimile: (205) 328-9669

JERROLD PARKER
Jerry@yourlawyer.com
PARKER WAICHMAN & ALONSO, LLP
6 Harbor Park Drive
Port Washington, NY 11050
Telephone: (516) 466-6500

FRED ROSENTHAL
frosenthal@yourlawyer.com
PARKER WAICHMAN & ALONSO, LLP
111 Great Neck Road,
Great Neck, NY 11021
Telephone: (516) 466-6500

JOHN GOODSON
KEIL & GOODSON
611 Pecan
Texarkana, TX 75501
Telephone: (870) 772-4113

ALAN MANSFIELD
alan@clgca.com
THE CONSUMER LAW GROUP
9466 Black Mountain Road
San Diego CA 92126
Telephone: (619) 308-5034

THOMAS MAURIELLO
tomm@maurlaw.com
MAURIELLO LAW FIRM APC
1181 Puerta Del Sol
San Clemente, CA 92673
Telephone: (949) 542-3555

DONALD CHIDI AMAMGBO
donald@amamgbolaw.com
AMAMGBO & ASSOCIATES
6167 Bristol Parkway
Culver City, CA 90230
Telephone: (310) 337-1137

REGINALD VON TERRELL
reggiet2@aol.com
THE TERRELL LAW GROUP
PO Box 13315
MPB # 148
Oakland CA 94661
Telephone: (510) 237-9700

GILLIAN L WADE
gwade@milsteinadelman.com
SARA D AVILA
savila@milsteinadelman.com
CORINA N. MACCARIN
MILSTEIN ADELMAN & KREGER LLP
2800 Donald Douglas Loop N
Santa Monica, CA 90405
Telephone: (310) 396-9600

RICHARD PROAPS
rproaps@aol.com
RICHARD ALAN PROAPS, ATTORNEY AT LAW
8150 Greenback Lane,
Fair Oaks, CA 95628
Telephone: (916) 722-4881

AARON C. MAYER
aaron@mayerlawgroup.com
MAYER LAW GROUP
18 Carolina St.
Charleston, SC 29403
Telephone: (843) 376-4929

HOWARD RUBINSTEIN
LAW OFFICES OF HOWARD W. RUBINSTEIN
1615 Forum Pl.
West Palm Beach, FL 33401
Telephone: (832) 715-2788;

BRIAN SMITH
bws@smithvanture.com
SMITH & VANTURE, LLP
1615 Forum Pl.
West Palm Beach, FL 33401
Telephone: (561) 684-6330

MONICA KELLY
monicakelly@ribbecklaw.com
RIBBECK LAW CHARTERED
505 North Lake Shore Drive
Chicago, IL 60611
Telephone: (312) 822-9999

ERIC QUETGLAS-JORDAN
eric@quetglaslaw.com
QUETGLAS LAW OFFICE
PO Box 16606
San Juan, PR 00908-6606
Telephone: (787) 722-7745

*Counsel for Plaintiffs*

**CERTIFICATE OF SERVICE**

I, David Stampley, an attorney, hereby certify that on November 21, 2011, I caused the above ***First Amended Consolidated Complaint*** and ***Jury Trial Demand***, to be served by causing true and accurate copies of such documents to be electronically filed and transmitted to counsel of record through the Court's CM/ECF electronic filing system.

Date: November 21, 2011

Respectfully submitted,
KAMBERLAW, LLC

By: s/David A. Stampley